Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide

Product and Documentation Release 9.0
August 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: 78-18394-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide, Release 9.0
Copyright © 2007–2012 Cisco Systems Inc. All rights reserved.

CONTENTS

Preface xxvii

Revision History xxvii

Document Objectives xxviii

Audience xxviii

Related Documentation xxviii

Document Conventions xxix

Obtaining Optical Networking Information xxxv

Where to Find Safety and Warning Information xxxv

Cisco Optical Networking Product Documentation CD-ROM xxxv

Obtaining Documentation and Submitting a Service Request xxxv

CHAPTER 1

General Troubleshooting 1-1

1.1 Network Troubleshooting Tests 1-2

1.1.1 Facility Loopback 1-2

1.1.2 Terminal Loopback 1-3

1.1.3 Hairpin Circuit 1-3

1.1.4 Cross-Connect Loopback 1-3

1.2 Identify Points of Failure on an Electrical Circuit Path 1-3

1.2.1 Perform a Facility Loopback on a Source-Node Port 1-4

Create the Facility Loopback on the Source-Node Port 1-4

Test the Facility Loopback 1-5

Test the Electrical Cabling 1-6

1.2.2 Perform a Hairpin on a Source-Node Port 1-6

Create the Hairpin on the Source-Node Port 1-6

Test the Hairpin Circuit 1-7

1.2.3 Perform a Terminal Loopback on a Destination-Node Port 1-7

Create the Terminal Loopback on a Destination-Node Port 1-7

Test the Terminal Loopback Circuit on the Destination-Node Port 1-9

1.2.4 Perform a Network Interface Unit Loopback on a Destination-Node Port 1-9

DS1 Inhibit FEAC Backplane Loopback 1-10

Create the NIU Loopback on a Destination-Node DS1 Port 1-10

Test and Clear the DS1 NIU Loopback Circuit 1-12

1.2.5 Perform a Hairpin Test on a Destination-Node Port 1-13

Create the Hairpin Loopback Circuit on the Destination-Node Port 1-13
Test the Hairpin Circuit 1-14
1.2.6 Perform a Facility Loopback on a Destination Port 1-14
Create a Facility Loopback Circuit on a Destination Port 1-14
Test the Facility Loopback Circuit 1-15
Test the Electrical Cabling 1-16
1.3 Identify Points of Failure on an OC-N Circuit Path 1-16
1.3.1 Perform a Facility Loopback on a Source-Node OC-N Port 1-17
Create the Facility Loopback on the Source OC-N Port 1-17
Test the Facility Loopback Circuit 1-17
1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port 1-18
Create the Cross-Connect Loopback on the Source OC-N Port 1-18
Test the Cross-Connect Loopback Circuit 1-19
1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port 1-19
Create the Terminal Loopback on a Source Node OC-N Port 1-19
Test the Terminal Loopback Circuit 1-20
1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port 1-21
Create the Facility Loopback on an Intermediate-Node OC-N Port 1-21
Test the Facility Loopback Circuit 1-22
1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port 1-22
Create the Terminal Loopback on an Intermediate-Node OC-N Port 1-23
Test the Terminal Loopback Circuit 1-24
1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port 1-24
Create the Facility Loopback on a Destination-Node OC-N Port 1-24
Test the Facility Loopback Circuit 1-25
1.3.7 Perform a Terminal Loopback on a Destination-Node OC-N Port 1-26
Create the Terminal Loopback on a Destination-Node OC-N Port 1-26
Test the Terminal Loopback Circuit 1-27
1.4 Troubleshooting Wideband Electrical Card(WBE-28 and WBE-84 Cards) FEAC on DS3 Ports 1-28
1.4.1 FEAC Send Code 1-29
1.4.2 WBE-28/WBE-84 Inhibit FEAC Loopback 1-29
1.4.3 FEAC Alarms 1-29
1.5 Troubleshooting WBE-28 and WBE-84 Cards with Far End Loopcodes on DS1 Ports 1-29
1.5.1 FEAC Send Code 1-30
1.5.2 WBE-28/WBE-84 Inhibit FEAC Loopback 1-30
1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks 1-31
1.6.1 Perform a Facility Loopback on a Source-Node Ethernet Port 1-31
Create the Facility Loopback on the Source-Node Ethernet Port 1-31
Test and Clear the Facility Loopback Circuit 1-32

Test the Ethernet Card 1-32
1.6.2 Perform a Terminal Loopback on a Source-Node Ethernet Port 1-33
Create the Terminal Loopback on a Source-Node Ethernet Port 1-33
Test and Clear the Ethernet Terminal Loopback Circuit 1-35
Test the Ethernet Card 1-35
1.6.3 Perform a Hairpin Test on a Source-Node Ethernet Port 1-36
Create the Hairpin Circuit on the Source-Node Ethernet Port 1-37
Test and Delete the Ethernet Port Hairpin Circuit 1-37
Test the Standby Cross-Connect Card 1-38
Retest the Original Cross-Connect Card 1-38
1.6.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port 1-39
Create a Facility Loopback on an Intermediate-Node OC-N Port 1-39
Test and Clear the OC-N Facility Loopback Circuit 1-40
Test the OC-N (Controller) Card 1-41
1.6.5 Perform a Terminal Loopback on Intermediate-Node OC-N Ports 1-42
Create a Terminal Loopback on Intermediate-Node OC-N Ports 1-42
Test and Clear the OC-N Terminal Loopback Circuit 1-43
Test the OC-N Card 1-44
1.6.6 Perform a Facility Loopback on a Destination-Node Ethernet Port 1-45
Create the Facility Loopback on a Destination-Node Ethernet Port 1-45
Test and Clear the Ethernet Facility Loopback Circuit 1-46
Test the Ethernet Card 1-47
1.6.7 Perform a Terminal Loopback on a Destination-Node Ethernet Port 1-48
Create the Terminal Loopback on a Destination-Node Ethernet Port 1-48
Test and Clear the Ethernet Terminal Loopback Circuit 1-49
Test the Ethernet Card 1-50
1.6.8 Perform a Hairpin Test on a Destination-Node Ethernet Port 1-51
Create the Hairpin Circuit on the Destination-Node Port 1-51
Test and Delete the Ethernet Hairpin Circuit 1-52
Test the Standby Cross-Connect Card 1-52
Retest the Original Cross-Connect Card 1-53
1.7 Verify Wiring from the ONS 15310-MA Shelf and DSX Wiring Panel 1-54
1.7.1 Set Up the Equipment for Testing 1-54
1.7.2 Perform Manual Mode Tests 1-57
1.7.2.1 Set Up the Handheld Receiver for Manual Mode Testing 1-57
1.7.2.2 Perform Manual Tests 1-57
1.7.2.3 View and Troubleshoot Manual Test Results 1-58
1.7.3 Perform Automatic Mode Tests 1-59
1.7.3.1 True Automatic Mode 1-59
1.7.3.2 Manual Prompt Mode 1-59

1.7.3.3 Provision the Handheld Receiver and Perform Automatic Mode Testing 1-60
1.7.3.4 View Automatic Mode Test Results During the Test 1-60
1.7.4 Retrieving Test Results from Automatic Tests 1-61
1.7.4.1 Reviewing the Results on the Handheld Receiver Screen 1-62
1.7.4.2 Sending the Results to a Computer 1-62
1.7.5 Perform Loop Tests 1-62
1.8 Restore the Database and Default Settings 1-63
1.8.1 Restore the Node Database 1-63
1.9 PC Connectivity Troubleshooting 1-63
1.9.1 Microsoft Windows PC System Minimum Requirements 1-64
1.9.2 Sun, Solaris, or UNIX System Minimum Requirements 1-64
1.9.3 Supported Platforms, Browsers, and JREs 1-64
1.9.4 Unsupported Platforms and Browsers 1-65
1.9.5 Unable to Verify the IP Configuration of Your Microsoft Windows PC 1-65
Verify the IP Configuration of Your Microsoft Windows PC 1-65
1.9.6 Browser Login Does Not Launch Java 1-66
Reconfigure the Microsoft Windows PC Operating System Java Plug-in Control Panel 1-66
Reconfigure the Browser 1-67
1.9.7 Unable to Verify the NIC Connection on Your Microsoft Windows PC 1-67
1.9.8 Verify Microsoft Windows PC Connection to the Node (Ping) 1-68
Ping the ONS 15310-CL or ONS 15310-MA 1-69
1.10 CTC Operation Troubleshooting 1-69
1.10.1 Unable to Launch CTC Help After Removing Netscape 1-69
Set Internet Explorer as the Default Browser for CTC 1-70
1.10.2 Unable to Change Node View to Network View 1-70
Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Microsoft Windows 1-70
Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris 1-71
1.10.3 Browser Stalls When Downloading CTC JAR Files from port 1-71
Disable the VirusScan Download Scan 1-72
1.10.4 CTC Does Not Launch 1-72
Redirect the Netscape Cache to a Valid Directory 1-72
1.10.5 Sluggish CTC Operation or Login Problems 1-73
Delete the CTC Cache File Automatically 1-73
Delete the CTC Cache File Manually 1-74
1.10.6 Node Icon is Gray on CTC Network View 1-74
1.10.7 Java Runtime Environment Incompatible 1-75
Launch CTC to Correct the Core Version Build 1-76
1.10.8 Different CTC Releases Do Not Recognize Each Other 1-76
Launch CTC to Correct the Core Version Build 1-76

1.10.9 Username or Password Does Not Match the Port Information 1-77
Verify Correct Username and Password 1-77
1.10.10 Superuser Password Needs to Be Reset 1-77
Reset the ONS 15310-CL or ONS 15310-MA Password 1-78
1.10.11 No IP Connectivity Exists Between Nodes 1-78
1.10.12 DCC Connection Lost 1-79
1.10.13 "Path in Use" Error When Creating a Circuit 1-79
Cancel the Circuit Creation and Start Over 1-79
1.10.14 Calculate and Design IP Subnets 1-80
1.11 Circuits and Timing 1-80
1.11.1 Circuit Transitions to Partial Status 1-80
View the State of Circuit Nodes 1-81
1.11.2 Circuits Remain in PARTIAL Status 1-81
1.11.3 AIS-V on Unused 15310-CL-CTX Card VT Circuits 1-82
Clear AIS-V on Unused Controller Card VT Circuits 1-82
1.11.4 Circuit Creation Error with VT1.5 Circuit 1-83
1.11.5 OC-3 and DCC Limitations 1-83
1.11.6 ONS 15310-CL or ONS 15310-MA Switches Timing Reference 1-83
1.11.7 Holdover Synchronization Alarm 1-84
1.11.8 Free-Running Synchronization Mode 1-85
1.11.9 Daisy-Chained BITS Not Functioning 1-85
1.11.10 Blinking STAT LED after Installing a Card 1-85
1.12 Fiber and Cabling 1-86
1.12.1 Bit Errors Appear for a Traffic Card 1-86
1.12.2 Faulty Fiber-Optic Connections 1-86
Verify Fiber-Optic Connections 1-87
1.12.2.1 Crimp Replacement LAN Cables 1-88
1.13 Power and LED Tests 1-90
1.13.1 Power Supply Problems 1-90
1.13.2 Power Consumption for Node and Cards 1-91
1.13.3 Lamp Tests for Card LEDs 1-91
Verify Card LED Operation 1-92
1.13.4 Retrieve Tech Support Logs Button 1-92
Off-Load the Diagnostics File 1-92

CHAPTER 2 **Alarm Troubleshooting** 2-1
2.1 Alarm Index by Default Severity 2-1
2.1.1 Critical Alarms (CR) 2-2
2.1.2 Major Alarms (MJ) 2-2

2.1.3 Minor Alarms (MN) 2-3
2.1.4 Not Alarmed Conditions 2-4
2.1.5 Not Reported (NR) Conditions 2-6
2.2 Alarms and Conditions Indexed By Alphabetical Entry 2-6
2.3 Alarm Logical Objects 2-10
2.4 Alarm List by Logical Object Type 2-12
2.5 Trouble Notifications 2-16
2.5.1 Alarm Characteristics 2-16
2.5.2 Condition Characteristics 2-16
2.5.3 Severities 2-17
2.5.4 Alarm Hierarchy 2-17
2.5.5 Service Effect 2-19
2.5.6 States 2-19
2.6 Safety Summary 2-19
2.7 Alarm Procedures 2-20
2.7.1 AIS 2-20
Clear the AIS Condition 2-21
2.7.2 AIS-L 2-21
Clear the AIS-L Condition 2-21
2.7.3 AIS-P 2-21
Clear the AIS-P Condition 2-21
2.7.4 AIS-V 2-22
Clear the AIS-V Condition 2-22
2.7.5 ALS 2-22
2.7.6 APC-END 2-22
2.7.7 APSB 2-22
Clear the APSB Alarm 2-23
2.7.8 APSCDFLTK 2-23
2.7.9 APSCINCON 2-23
Clear the APSCINCON Alarm 2-23
2.7.10 APSCM 2-23
Clear the APSCM Alarm 2-24
2.7.11 APSCNMIS 2-24
2.7.12 APSIMP 2-24
Clear the APSIMP Alarm 2-25
2.7.13 APS-INV-PRIM 2-25
2.7.14 APSMM 2-25
Clear the APSMM Alarm 2-26
2.7.15 APS-PRIM-FAC 2-27

Clear the APS-PRIM-FAC Condition 2-27
2.7.16 APS-PRIM-SEC-MISM 2-27
Clear the APS-PRIM-SEC-MISM Alarm 2-27
2.7.17 AS-CMD 2-27
Clear the AS-CMD Condition 2-28
2.7.18 AS-MT 2-29
Clear the AS-MT Condition 2-29
2.7.19 AS-MT-OOG 2-29
2.7.20 AUD-LOG-LOSS 2-29
Clear the AUD-LOG-LOSS Condition 2-29
2.7.21 AUD-LOG-LOW 2-30
2.7.22 AUTOLSROFF 2-30
2.7.23 AUTORESET 2-30
Clear the AUTORESET Alarm 2-30
2.7.24 AUTOSW-AIS 2-31
Clear the AUTOSW-AIS Condition 2-31
2.7.25 AUTOSW-LOP (STSMON) 2-32
Clear the AUTOSW-LOP (STSMON) Condition 2-32
2.7.26 AUTOSW-LOP (VT-MON) 2-32
Clear the AUTOSW-LOP (VT-MON) Alarm 2-32
2.7.27 AUTOSW-PDI 2-32
Clear the AUTOSW-PDI Condition 2-33
2.7.28 AUTOSW-SDBER 2-33
Clear the AUTOSW-SDBER Condition 2-33
2.7.29 AUTOSW-SFBER 2-33
Clear the AUTOSW-SFBER Condition 2-34
2.7.30 AUTOSW-UNEQ (STSMON) 2-34
Clear the AUTOSW-UNEQ (STSMON) Condition 2-34
2.7.31 AUTOSW-UNEQ (VT-MON) 2-34
Clear the AUTOSW-UNEQ (VT-MON) Alarm 2-35
2.7.32 BAT-FAIL 2-35
Clear the BAT-FAIL Alarm 2-35
2.7.33 BERT-ENBL 2-36
2.7.34 BERT-SYNC-FAIL 2-36
2.7.35 BKUPMEMP 2-36
Clear the BKUPMEMP Alarm 2-36
2.7.36 BLSROSYNC 2-37
2.7.37 CARLOSS (CE100T, CEMR) 2-37
Clear the CARLOSS (CE100T, CEMR) Alarm 2-37
2.7.38 CARLOSS (EQPT) 2-39

Clear the CARLOSS (EQPT) Alarm 2-39
2.7.39 CARLOSS (ML100T) 2-40
Clear the CARLOSS (ML100T) Alarm 2-41
2.7.40 CLDRESTART 2-41
Clear the CLDRESTART Condition 2-42
2.7.41 COMIOXC 2-42
Clear the COMIOXC Alarm 2-42
2.7.42 CONTBUS-CLK-A 2-43
Clear the CONTBUS-CLK-A Alarm 2-43
2.7.43 CONTBUS-CLK-B 2-43
Clear the CONTBUS-CLK-B Alarm 2-43
2.7.44 CONTBUS-DISABLED 2-44
Clear the CONTBUS-DISABLED Alarm 2-44
2.7.45 CONTBUS-IO-A 2-45
Clear the CONTBUS-IO-A Alarm 2-45
2.7.46 CONTBUS-IO-B 2-45
2.7.47 CTNEQPT-PBPROT 2-46
Clear the CTNEQPT-PBPROT Alarm 2-46
2.7.48 CTNEQPT-PBWORK 2-47
Clear the CTNEQPT-PBWORK Alarm 2-47
2.7.49 DATA-CRC; 2-48
Clear the DATA-CRC Alarm 2-48
2.7.50 DATAFLT 2-48
Clear the DATAFLT Alarm 2-49
2.7.51 DBOSYNC 2-49
Clear the DBOSYNC Alarm 2-49
2.7.52 DISCONNECTED 2-49
Clear the DISCONNECTED Alarm 2-50
2.7.53 DS3-MISM 2-50
Clear the DS3-MISM Condition 2-50
2.7.54 DUP-IPADDR 2-50
Clear the DUP-IPADDR Alarm 2-51
2.7.55 DUP-NODENAME 2-51
Clear the DUP-NODENAME Alarm 2-51
2.7.56 DUP-SHELF-ID 2-52
2.7.57 EHIBATVG 2-52
Clear the EHIBATVG Alarm 2-52
2.7.58 ELWBATVG 2-52
Clear the ELWBATVG Alarm 2-52
2.7.59 ENCAP-MISMATCH-P 2-53

Clear the ENCAP-MISMATCH-P Alarm 2-54
2.7.60 EOC 2-54
Clear the EOC Alarm 2-55
2.7.61 EOC-L 2-56
Clear the EOC-L Alarm 2-57
2.7.62 EQPT 2-57
Clear the EQPT Alarm 2-57
2.7.63 EQPT-MISS 2-58
2.7.64 ERFI-P-CONN 2-58
Clear the ERFI-P-CONN Condition 2-58
2.7.65 ERFI-P-PAYLD 2-59
Clear the ERFI-P-PAYLD Condition 2-59
2.7.66 ERROR-CONFIG 2-59
Clear the ERROR-CONFIG Alarm 2-59
2.7.67 ETH-LINKLOSS 2-60
Clear the ETH-LINKLOSS Condition 2-61
2.7.68 EXCCOL 2-61
Clear the EXCCOL Alarm 2-61
2.7.69 EXT 2-61
Clear the EXT Alarm 2-61
2.7.70 FAILTOSW 2-62
Clear the FAILTOSW Condition 2-62
2.7.71 FAILTOSW-PATH 2-62
Clear the FAILTOSW-PATH Condition in a Path Protection Configuration 2-62
2.7.72 FAN 2-63
2.7.73 FAN-DEGRADE 2-63
2.7.74 FE-AIS 2-63
Clear the FE-AIS Condition 2-64
2.7.75 FE-DS1-MULTLOS 2-64
Clear the FE-DS1-MULTLOS Condition 2-64
2.7.76 FE-DS1-NSA 2-64
Clear the FE-DS1-NSA Condition 2-64
2.7.77 FE-DS1-SA 2-65
Clear the FE-DS1-SA Condition 2-65
2.7.78 FE-DS1-SNGLLOS 2-65
Clear the FE-DS1-SNGLLOS Condition 2-65
2.7.79 FE-DS3-NSA 2-66
Clear the FE-DS3-NSA Condition 2-66
2.7.80 FE-DS3-SA 2-66
Clear the FE-DS3-SA Condition 2-66

2.7.81 FE-EQPT-NSA 2-67
Clear the FE-EQPT-NSA Condition 2-67
2.7.82 FE-FRCDWKSWBK-SPAN 2-67
Clear the FE-FRCDWKSWBK-SPAN Condition 2-67
2.7.83 FE-FRCDWKSWPR-SPAN 2-68
2.7.84 FE-IDLE 2-68
Clear the FE-IDLE Condition 2-68
2.7.85 FE-LOCKOUTOFPR-SPAN 2-68
2.7.86 FE-LOF 2-68
Clear the FE-LOF Condition 2-68
2.7.87 FE-LOS 2-69
Clear the FE-LOS Condition 2-69
2.7.88 FE-MANWKSWBK-SPAN 2-69
2.7.89 FE-MANWKSWPR-SPAN 2-69
2.7.90 FEPRLF 2-69
Clear the FEPRLF Alarm 2-70
2.7.91 FORCED-REQ 2-70
Clear the FORCED-REQ Condition 2-70
2.7.92 FORCED-REQ-SPAN 2-70
Clear the FORCED-REQ-SPAN Condition 2-70
2.7.93 FP-LINK-LOSS 2-71
2.7.94 FRCDSWTOINT 2-71
2.7.95 FRCDSWTOPRI 2-71
2.7.96 FRCDSWTOSEC 2-71
2.7.97 FRCDSWTOTHIRD 2-72
2.7.98 FRNGSYNC 2-72
Clear the FRNGSYNC Condition 2-72
2.7.99 FSTSYNC 2-72
2.7.100 FULLPASSTHR-BI 2-73
2.7.101 GFP-CSF 2-73
Clear the GFP-CSF Alarm 2-73
2.7.102 GFP-EX-MISMATCH 2-73
Clear the GFP-EX-MISMATCH Alarm 2-74
2.7.103 GFP-LFD 2-74
Clear the GFP-LFD Alarm 2-74
2.7.104 GFP-UP-MISMATCH 2-74
Clear the GFP-UP-MISMATCH Alarm 2-75
2.7.105 HELLO 2-75
Clear the HELLO Alarm 2-75
2.7.106 HIBATVG 2-76

Clear the HIBATVG Alarm 2-76
2.7.107 HI-LASERBIAS 2-76
Clear the HI-LASERBIAS Alarm 2-76
2.7.108 HI-LASERTEMP 2-77
Clear the HI-LASERTEMP Alarm 2-77
2.7.109 HI-RXPOWER 2-78
Clear the HI-RXPOWER Alarm 2-78
2.7.110 HITEMP 2-78
Clear the HITEMP Alarm 2-78
2.7.111 HI-TXPOWER 2-78
Clear the HI-TXPOWER Alarm 2-79
2.7.112 HLDOVRSYNC 2-79
Clear the HLDOVRSYNC Alarm 2-80
2.7.113 I-HITEMP 2-80
Clear the I-HITEMP Alarm 2-80
2.7.114 IMPROPRMVL 2-81
Clear the IMPROPRMVL Alarm 2-81
2.7.115 INC-ISD 2-82
2.7.116 INCOMPATIBLE-SEND-PDIP 2-83
Clear the INCOMPATIBLE-SEND-PDIP Alarm 2-83
2.7.117 INCOMPATIBLE-SW 2-83
Clear the INCOMPATIBLE-SW Alarm 2-83
2.7.118 INHSWPR 2-83
Clear the INHSWPR Condition 2-84
2.7.119 INHSWWKG 2-84
2.7.120 INTRUSION-PSWD 2-84
Clear the INTRUSION-PSWD Condition 2-84
2.7.121 INVMACADR 2-85
2.7.122 IOSCFGCOPY 2-85
2.7.123 ISIS-ADJ-FAIL 2-85
Clear the ISIS-ADJ-FAIL Alarm 2-86
2.7.124 KB-PASSTHR 2-87
2.7.125 LASEREOL 2-87
2.7.126 LCAS-CRC 2-87
Clear the LCAS-CRC Condition 2-88
2.7.127 LCAS-RX-DNU 2-88
Clear the LCAS-RX-DNU Condition 2-88
2.7.128 LCAS-RX-FAIL 2-89
Clear the LCAS-RX-FAIL Condition 2-89
2.7.129 LCAS-TX-ADD 2-89

2.7.130 LCAS-TX-DNU 2-90
2.7.131 LINK-KEEPALIVE 2-90
Clear the LINK-KEEPALIVE Alarm 2-91
2.7.132 LKOUTPR-S 2-91
Clear the LKOUTPR-S Condition 2-91
2.7.133 LOA 2-91
Clear the LOA Alarm 2-92
2.7.134 LOCKOUT-REQ 2-92
Clear the LOCKOUT-REQ Condition 2-92
2.7.135 LOF (BITS) 2-92
Clear the LOF (BITS) Alarm 2-93
2.7.136 LOF (DS1) 2-93
Clear the LOF (DS1) Alarm 2-94
2.7.137 LOF (DS3) 2-94
Clear the LOF (DS3) Alarm 2-94
2.7.138 LOF (EC1) 2-95
Clear the LOF (EC1) Alarm 2-95
2.7.139 LOF (OCN) 2-95
Clear the LOF (OCN) Alarm 2-96
2.7.140 LOF (STSTRM) 2-96
Clear the LOF (STSTRM) Alarm 2-96
2.7.141 LOGBUFR90 2-96
2.7.142 LOGBUFROVFL 2-96
Clear the LOGBUFROVFL Alarm 2-97
2.7.143 LO-LASERBIAS 2-97
Clear the LO-LASERBIAS Alarm 2-97
2.7.144 LO-LASERTEMP 2-98
2.7.145 LOM 2-98
Clear the LOM Alarm 2-98
2.7.146 LOP-P 2-98
Clear the LOP-P Alarm 2-99
2.7.147 LOP-V 2-99
Clear the LOP-V Alarm 2-99
2.7.148 LO-RXPOWER 2-99
Clear the LO-RXPOWER Alarm 2-100
2.7.149 LOS (BITS) 2-101
Clear the LOS (BITS) Alarm 2-101
2.7.150 LOS (DS1) 2-101
Clear the LOS (DS1) Alarm 2-101
2.7.151 LOS (DS3) 2-102

Clear the LOS (DS3) Alarm 2-103
2.7.152 LOS (EC1) 2-104
Clear the LOS (EC1) Alarm 2-104
2.7.153 LOS (FUDC) 2-105
Clear the LOS (FUDC) Alarm 2-105
2.7.154 LOS (OCN) 2-106
Clear the LOS (OCN) Alarm 2-106
2.7.155 LO-TXPOWER 2-107
Clear the LO-TXPOWER Alarm 2-107
2.7.156 LPBKCRS 2-108
Clear the LPBKCRS Condition 2-108
2.7.157 LPBKDS3FEAC 2-108
Clear the LPBKDS3FEAC Condition 2-109
2.7.158 LPBKDS3FEAC-CMD 2-109
2.7.159 LPBKFACILITY (CE100T, CEMR) 2-109
Clear the LPBKFACILITY (CE100T, CEMR) Condition 2-109
2.7.160 LPBKFACILITY (DS1, DS3) 2-109
Clear the LPBKFACILITY (DS1, DS3) Condition 2-110
2.7.161 LPBKFACILITY (EC1) 2-110
Clear the LPBKFACILITY (EC1) Condition 2-110
2.7.162 LPBKFACILITY (OCN) 2-111
Clear the LPBKFACILITY (OCN) Condition 2-111
2.7.163 LPKTERMINAL (CE100T, CEMR) 2-111
Clear the LPBKTERMINAL (CE100T, CEMR) Condition 2-111
2.7.164 LPBKTERMINAL (DS1, DS3) 2-112
Clear the LPBKTERMINAL (DS1, DS3) Condition 2-112
2.7.165 LPBKTERMINAL (EC1) 2-112
Clear the LPBKTERMINAL (EC1) Condition 2-112
2.7.166 LPBKTERMINAL (OCN) 2-113
Clear the LPBKTERMINAL (OCN) Condition 2-113
2.7.167 LWBATVG 2-113
Clear the LWBATVG Alarm 2-113
2.7.168 MAN-REQ 2-114
Clear the MAN-REQ Condition 2-114
2.7.169 MANRESET 2-114
2.7.170 MANSWTOINT 2-114
2.7.171 MANSWTOPRI 2-114
2.7.172 MANSWTOSEC 2-115
2.7.173 MANSWTOTHIRD 2-115
2.7.174 MANUAL-REQ-SPAN 2-115

Clear the MANUAL-REQ-SPAN Condition 2-115
2.7.175 MATECLK 2-116
Clear the MATECLK Alarm 2-116
2.7.176 MEA (EQPT) 2-116
Clear the MEA (EQPT) Alarm 2-116
2.7.177 MEA (FAN) 2-117
2.7.178 MEA (PPM) 2-118
2.7.179 MEA (SHELF) 2-118
2.7.180 MEM-GONE 2-118
2.7.181 MEM-LOW 2-118
2.7.182 MFGMEM 2-118
2.7.183 NO-CONFIG 2-119
Clear the NO-CONFIG Condition 2-119
2.7.184 NON-CISCO-PPM 2-119
Clear the NON-CISCO-PPM Condition 2-120
2.7.185 NOT-AUTHENTICATED 2-120
2.7.186 OOU-TPT 2-120
Clear the OOT-TPT Condition 2-120
2.7.187 OPEN-SLOT 2-120
Clear the OPEN-SLOT Condition 2-121
2.7.188 PDI-P 2-121
Clear the PDI-P Condition 2-122
2.7.189 PLM-P 2-122
Clear the PLM-P Alarm 2-123
2.7.190 PLM-V 2-123
Clear the PLM-V Alarm 2-123
2.7.191 PORT-MISMATCH 2-123
2.7.192 PRC-DUPID 2-124
2.7.193 PROTNA 2-124
Clear the PROTNA Alarm 2-124
2.7.194 PROV-MISMATCH 2-124
2.7.195 PWR-FAIL-A 2-125
Clear the PWR-FAIL-A Alarm 2-125
2.7.196 PWR-FAIL-B 2-125
Clear the PWR-FAIL-B Alarm 2-126
2.7.197 RAI 2-126
Clear the RAI Condition 2-126
2.7.198 RFI-L 2-126
Clear the RFI-L Condition 2-126
2.7.199 RFI-P 2-127

Clear the RFI-P Condition 2-127
2.7.200 RFI-V 2-127
Clear the RFI-V Condition 2-128
2.7.201 ROLL 2-128
2.7.202 ROLL-PEND 2-129
2.7.203 ROUTE-OVERFLOW 2-129
Clear the ROUTE-OVERFLOW Condition 2-129
2.7.204 RPR-PASSTHR 2-129
2.7.205 RPRW 2-129
Clear the RPRW Condition 2-130
2.7.206 RUNCFG-SAVENEED 2-130
2.7.207 SD 2-130
Clear the SD (DS1, DS3) Condition 2-131
2.7.208 SD-L 2-132
Clear the SD-L Condition 2-132
2.7.209 SD-P 2-133
Clear the SD-P Condition 2-133
2.7.210 SD-V 2-133
Clear the SD-V Condition 2-133
2.7.211 SF 2-134
Clear the SF (DS1, DS3) Condition 2-134
2.7.212 SF-L 2-134
Clear the SF-L Condition 2-135
2.7.213 SF-P 2-135
Clear the SF-P Condition 2-135
2.7.214 SFTWDOWN 2-135
2.7.215 SF-V 2-135
Clear the SF-V Condition 2-136
2.7.216 SHELF-COMM-FAIL 2-136
2.7.217 SNTP-HOST 2-136
Clear the SNTP-HOST Alarm 2-136
2.7.218 SQM 2-137
Clear the SQM Alarm 2-137
2.7.219 SSM-DUS 2-137
2.7.220 SSM-FAIL 2-137
Clear the SSM-FAIL Alarm 2-138
2.7.221 SSM-LNC 2-138
2.7.222 SSM-OFF 2-138
Clear the SSM-OFF Condition 2-138
2.7.223 SSM-PRC 2-138

2.7.224 SSM-PRS 2-139
2.7.225 SSM-RES 2-139
2.7.226 SSM-SDH-TN 2-139
2.7.227 SSM-SETS 2-139
2.7.228 SSM-SMC 2-139
2.7.229 SSM-ST2 2-140
2.7.230 SSM-ST3 2-140
2.7.231 SSM-ST3E 2-140
2.7.232 SSM-ST4 2-140
2.7.233 SSM-STU 2-141
Clear the SSM-STU Condition 2-141
2.7.234 SSM-TNC 2-141
2.7.235 SW-MISMATCH 2-141
Clear the SW-MISMATCH Condition 2-141
2.7.236 SWMTXMOD-PROT 2-142
Clear the SWMTXMOD-PROT Alarm 2-142
2.7.237 SWMTXMOD-WORK 2-142
Clear the SWMTXMOD-WORK Alarm 2-142
2.7.238 SWTOPRI 2-143
2.7.239 SWTOSEC 2-143
Clear the SWTOSEC Condition 2-143
2.7.240 SWTOTHIRD 2-143
Clear the SWTOTHIRD Condition 2-144
2.7.241 SYNC-FREQ 2-144
Clear the SYNC-FREQ Condition 2-144
2.7.242 SYNCPRI 2-144
Clear the SYNCPRI Alarm 2-144
2.7.243 SYNCSEC 2-145
Clear the SYNCSEC Alarm 2-145
2.7.244 SYNCTHIRD 2-145
Clear the SYNCTHIRD Alarm 2-146
2.7.245 SYSBOOT 2-146
2.7.246 TIM 2-146
Clear the TIM Alarm 2-147
2.7.247 TIM-MON 2-147
2.7.248 TIM-P 2-148
Clear the TIM-P Alarm 2-148
2.7.249 TIM-S 2-148
Clear the TIM-S Alarm 2-149
2.7.250 TIM-V 2-149

Clear the TIM-V Alarm 2-149
2.7.251 TPTFAIL 2-149
Clear the TPTFAIL Alarm 2-149
2.7.252 TX-AIS 2-150
Clear the TX-AIS Condition 2-150
2.7.253 TX-LOF 2-150
Clear the TX-LOF Condition 2-150
2.7.254 TX-RAI 2-151
Clear the TX-RAI Condition 2-151
2.7.255 UNEQ-P 2-151
Clear the UNEQ-P Alarm 2-151
2.7.256 UNEQ-V 2-153
Clear the UNEQ-V Alarm 2-153
2.7.257 UNQUAL-PPM 2-153
Clear the UNQUAL-PPM Condition 2-153
2.7.258 VCG-DEG 2-154
Clear the VCG-DEG Condition 2-154
2.7.259 VCG-DOWN 2-154
Clear the VCG-DOWN Condition 2-154
2.7.260 WKSWPR 2-155
Clear the WKSWPR Condition 2-155
2.7.261 WTR 2-155
2.8 DS-1 Line Alarms 2-155
2.9 Traffic Card LED Activity 2-156
2.9.1 Typical Controller Card or Ethernet Card LED Activity After Insertion 2-156
2.9.2 Typical Card LED Activity During Reset 2-156
2.10 Frequently Used Alarm Troubleshooting Procedures 2-156
2.10.1 Protection Switching, Lock Initiation, and Clearing 2-156
Initiate a 1+1 Protection Port Force Switch Command 2-157
Initiate a 1+1 Manual Switch Command 2-157
Clear a 1+1 Force or Manual Switch Command 2-158
Initiate a Lock-On Command 2-158
Initiate a Card or Port Lockout Command 2-159
Clear a Lock-On or Lockout Command 2-159
Initiate an ONS 15310-MA 1:1 Card Switch Command 2-159
Initiate a Force Switch for All Circuits on a Path Protection Span 2-160
Initiate a Manual Switch for All Circuits on a Path Protection Span 2-160
Initiate a Lockout for All Circuits on a Protect Path Protection Span 2-161
Clear an External Switching Command on a Path Protection Span 2-161

2.10.2 CTC Card Resetting and Switching 2-162
Soft- or Hard-Reset an Ethernet or Electrical Card in CTC 2-162
Soft- or Hard-Reset a Controller Card 2-162
2.10.3 Physical Card Reseating and Replacement 2-163
Remove and Reinsert (Reseat) a Card 2-163
Physically Replace a Card 2-163
2.10.4 Generic Signal and Circuit Procedures 2-164
Verify the Signal BER Threshold Level 2-164
Delete a Circuit 2-164
Verify or Create Node DCC Terminations 2-164
Clear an OC-N Port Facility or Terminal Loopback Circuit 2-165
Clear an OC-N Port XC Loopback Circuit 2-165
Clear a DS-3 or DS-1 Port Loopback Circuit 2-165
Clear an EC-1 Port Loopback 2-166
Clear an Ethernet Card Loopback Circuit 2-166

CHAPTER 3 **Transient Conditions** 3-1

3.1 Transients Indexed By Alphabetical Entry 3-1
3.2 Trouble Notifications 3-3
3.2.1 Condition Characteristics 3-3
3.2.2 Condition States 3-4
3.3 Transient Conditions 3-4
3.3.1 ADMIN-DISABLE 3-4
3.3.2 ADMIN-DISABLE-CLR 3-4
3.3.3 ADMIN-LOCKOUT 3-4
3.3.4 ADMIN-LOCKOUT-CLR 3-4
3.3.5 ADMIN-LOGOUT 3-5
3.3.6 ADMIN-SUSPEND 3-5
3.3.7 ADMIN-SUSPEND-CLR 3-5
3.3.8 AUD-ARCHIVE-FAIL 3-5
3.3.9 DBBACKUP-FAIL 3-5
3.3.10 DBRESTORE-FAIL 3-5
3.3.11 EFM-ERR-FRM 3-6
3.3.12 EFM-FRM-PER 3-6
3.3.13 EFM-FRM-SEC 3-6
3.3.14 EFM-RLBK-FAIL 3-6
3.3.15 EFM-SYM-PER 3-6
3.3.16 FIREWALL-DIS 3-6
3.3.17 FRCDWKSWBK-NO-TRFSW 3-7

3.3.18 FRCDWKSWPR-NO-TRFSW 3-7
3.3.19 INTRUSION 3-7
3.3.20 INTRUSION-PSWD 3-7
3.3.21 LOGIN-FAIL-LOCKOUT 3-7
3.3.22 LOGIN-FAIL-ONALRDY 3-7
3.3.23 LOGIN-FAILURE-PSWD 3-7
3.3.24 LOGIN-FAILURE-USERID 3-8
3.3.25 LOGOUT-IDLE-USER 3-8
3.3.26 MANWKSWBK-NO-TRFSW 3-8
3.3.27 MANWKSWPR-NO-TRFSW 3-8
3.3.28 PM-TCA 3-8
3.3.29 PS 3-8
3.3.30 RMON-ALARM 3-9
3.3.31 RMON-RESET 3-9
3.3.32 SESSION-TIME-LIMIT 3-9
3.3.33 SFTWDOWN-FAIL 3-9
3.3.34 USER-LOCKOUT 3-9
3.3.35 USER-LOGIN 3-9
3.3.36 USER-LOGOUT 3-9
3.3.37 WORK-QUEUE-FULL 3-10
3.3.38 WKSWBK 3-10
3.3.39 WKSWPR 3-10
3.3.40 WRMRESTART 3-10

CHAPTER 4 **Error Messages** 4-1

INDEX

FIGURES

Figure 1-1 Accessing FEAC Functions on the DS1 ports of WBE-28/WBE-84 Cards **1-11**

Figure 1-2 Diagram of FEAC Circuit **1-11**

Figure 1-3 Accessing FEAC Functions on the DS3 ports of WBE-28/WBE-84 Cards **1-28**

Figure 1-4 Diagram of FEAC Circuit **1-29**

Figure 1-5 Accessing Far End troubleshooting Functions on the WBE Cards **1-30**

Figure 1-6 Hairpin Loopback on a Source-Node Ethernet Port **1-36**

Figure 1-7 Hairpin on a Destination-Node Ethernet Port **1-51**

Figure 1-8 TST-DSX and Remote Receiver Faceplates **1-55**

Figure 1-9 Handheld Receiver Usage Flowchart **1-56**

Figure 1-10 Deleting the CTC Cache **1-74**

Figure 1-11 RJ-45 Pin Numbers **1-88**

Figure 1-12 LAN Cable Layout **1-89**

Figure 1-13 Cross-Over Cable Layout **1-89**

Figure 4-1 Error Dialog Box **4-1**

TABLES

Table 1-1 Messages and Probable Indications **1-58**

Table 1-2 Automatic Test Mode Results **1-61**

Table 1-3 Restore the Node Database **1-63**

Table 1-4 Unable to Verify the IP Configuration of Your Microsoft Windows PC **1-65**

Table 1-5 Browser Login Does Not Launch Java **1-66**

Table 1-6 Unable to Verify the NIC Connection on Your Microsoft Windows PC **1-68**

Table 1-7 Verify Microsoft Windows PC Connection to ONS 15310-CL or ONS 15310-MA (Ping) **1-68**

Table 1-8 Unable to Launch CTC Help After Removing Netscape **1-69**

Table 1-9 Unable to Change Node View to Network View **1-70**

Table 1-10 Browser Stalls When Downloading JAR File from Port **1-71**

Table 1-11 CTC Does Not Launch **1-72**

Table 1-12 Sluggish CTC Operation or Login Problems **1-73**

Table 1-13 Node Icon is Gray on CTC Network View **1-75**

Table 1-14 Java Runtime Environment Incompatible **1-75**

Table 1-15 Different CTC Releases Do Not Recognize Each Other **1-76**

Table 1-16 Username or Password Does Not Match the Port Information **1-77**

Table 1-17 No IP Connectivity Exists Between Nodes **1-78**

Table 1-18 No IP Connectivity Exists Between Nodes **1-79**

Table 1-19 DCC Connection Lost **1-79**

Table 1-20 "Path in Use" Error When Creating a Circuit **1-79**

Table 1-21 Calculate and Design IP Subnets **1-80**

Table 1-22 Circuit in Partial Status **1-81**

Table 1-23 Circuits Remain in PARTIAL Status **1-81**

Table 1-24 AIS-V on Unused 15310-CL-CTX Card VT Circuits **1-82**

Table 1-25 Circuit Creation Error with VT1.5 Circuit **1-83**

Table 1-26 OC-3 and DCC Limitations **1-83**

Table 1-27 ONS 15310-CL or ONS 15310-MA Switches Timing Reference **1-84**

Table 1-28 Holdover Synchronization Alarm **1-84**

Table 1-29 Free-Running Synchronization Mode **1-85**

Table 1-30 Daisy-Chained BITS Not Functioning **1-85**

Table 1-31 Blinking STAT LED on Installed Card **1-85**
Table 1-32 Bit Errors Appear for a Line Card **1-86**
Table 1-33 Faulty Fiber-Optic Connections **1-86**
Table 1-34 LAN Cable Pinout **1-89**
Table 1-35 Cross-Over Cable Pinout **1-89**
Table 1-36 Power Supply Problems **1-90**
Table 1-37 Power Consumption for Node and Cards **1-91**
Table 1-38 Lamp Test for Optical and Electrical Card LEDs **1-91**
Table 1-39 Diagnostic Files Retrieved Based on User Privilege **1-93**
Table 1-40 List of Diagnostic Files **1-94**
Table 2-1 ONS 15310-CL and ONS 15310-MA Critical Alarm List **2-2**
Table 2-2 ONS 15310-CL and ONS 15310-MA Major Alarm List **2-2**
Table 2-3 ONS 15310-CL and ONS 15310-MA Minor Alarm List **2-3**
Table 2-4 ONS 15310-CL and ONS 15310-MA NA Conditions List **2-4**
Table 2-5 ONS 15310-CL and ONS 15310-MA Major Alarm List **2-6**
Table 2-6 ONS 15310-CL and ONS 15310-MA Alarm and Condition Alphabetical List **2-6**
Table 2-7 Alarm Logical Object Type Definitions **2-11**
Table 2-8 ONS 15310-CL and ONS 15310-MA Alarm List by Logical Object as Shown in Alarm Profile **2-12**
Table 2-9 Path Alarm Hierarchy **2-17**
Table 2-10 Facility Alarm Hierarchy **2-18**
Table 2-11 Near-End Alarm Hierarchy **2-18**
Table 2-12 Far-End Alarm Hierarchy **2-19**
Table 2-13 DS-1 Alarms by Line Type **2-155**
Table 3-1 ONS 15310-CL and ONS 15310-MA Transient Condition Alphabetical List **3-1**
Table 4-1 Error Messages **4-2**

Preface

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This section explains the objectives, intended audience, and organization of this troubleshooting guide and describes the conventions that convey instructions and other information.

This section provides the following information:

- Revision History
- Document Objectives
- Audience
- Related Documentation
- Document Conventions
- Obtaining Optical Networking Information
- Obtaining Documentation and Submitting a Service Request

Revision History

Date	Notes
January 2009	Updated the extreme high, extreme low, high and low voltage values in sections 2.7.57 EHIBATVG, 2.7.58 ELWBATVG, 2.7.106 HIBATVG, and 2.7.167 LWBATVG in Chapter 2, Alarm Troubleshooting.
May 2009	Updated PWR-FAIL-A alarm details in Chapter 2, Alarm Troubleshooting.
June 2009	Updated PWR-FAIL-B alarm details in Chapter 2, Alarm Troubleshooting.
August 2009	Updated MEM-GONE alarm description in Chapter 2, Alarm Troubleshooting.
November 2009	Updated the card details for LCAS alarms in Chapter 2, Alarm Troubleshooting.

Date	Notes
June 2010	Updated the table “Alarm Logical Object Type Definitions” in the chapter “Alarm Troubleshooting”.
July 2010	Updated table in Chapter Error Messages.
February 2012	Updated the section “IMPROPRMVL” in the chapter “Alarm Troubleshooting”.
August 2012	The full length book-PDF was generated.

Document Objectives

This guide gives general troubleshooting instructions, alarm troubleshooting instructions, equipment replacement instructions, and a list of error messages that apply to the ONS 15310-CL equipment. This information is contained in four chapters. Use this guide in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

To use this publication, you should be familiar with Cisco or equivalent optical transmission hardware and cabling, telecommunications hardware and cabling, electronic circuitry and wiring practices, and preferably have experience as a telecommunications technician.

Related Documentation

Use the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Troubleshooting Guide* in conjunction with the following publications:

- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide, Release 9.0*
  Provides installation, turn up, test, and maintenance procedures.
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual, Release 9.0*
  Provides detailed card specifications, hardware and software feature descriptions, network topology information, and network element defaults.
- *Cisco ONS SONET TL1 Command Guide, Release 9.0*
  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15454, ONS 15600, ONS 15310-CL, and ONS 15310-MA systems.
- *Cisco ONS SONET TL1 Reference Guide, Release 9.0*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454, ONS 15600, ONS 15310-CL, and ONS 15310-MA systems.
- *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide, Release 9.0*
  Provides software feature and operation information for Ethernet cards in the Cisco ONS 15310-CL and Cisco ONS 15310-MA.
- *Release Notes for the Cisco ONS 15310-CL Release 9.0*
  Provides caveats, closed issues, and new feature and functionality information.

- *Release Notes for the Cisco ONS 15310-MA Release 9.0*
  Provides caveats, closed issues, and new feature and functionality information.

Refer to the following standards documentation referenced in this publication:

- Telcordia GR-253 CORE

For an update on End-of-Life and End-of-Sale notices, refer to http://www.cisco.com/en/US/products/hw/optical/ps2001/prod_eol_notices_list.html.

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
italic	Command input that is supplied by the user.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information that the user must enter.
< >	Command parameters that must be replaced by module-specific codes.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, the user might do something that could result in equipment damage or loss of data.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

FONTOS BIZTONSÁGI ELOÍRÁSOK

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير **إرشادات الأمان الهامة**

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.

قم بحفظ هذه الإرشادات

Upozorenje **VAŽNE SIGURNOSNE NAPOMENE**

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění **DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY**

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Obtaining Optical Networking Information

This section contains information that is specific to optical networking products. For information that pertains to all of Cisco, refer to the Obtaining Documentation and Submitting a Service Request section.

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15454 system. It also includes translations of the safety warnings that appear in the ONS 15454 system documentation.

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

General Troubleshooting

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15310-CL or Cisco ONS 15310-MA. To troubleshoot specific alarms, see Chapter 2, "Alarm Troubleshooting."

This chapter includes the following sections on network problems:

- 1.1 Network Troubleshooting Tests—Describes loopbacks and hairpin circuits, which you can use to test circuit paths through the network or logically isolate faults.

Note For network acceptance tests, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

- 1.2 Identify Points of Failure on an Electrical Circuit Path—Explains how to perform loopback and hairpin tests, which you can use to test ONS 15310-CL DS-N circuit paths through the network or logically isolate faults.
- 1.3 Identify Points of Failure on an OC-N Circuit Path—Explains how to perform loopback and hairpin tests on OC-N paths, which you can use to test ONS 15310-CL or ONS 15310-MA OC-N circuit paths through the network or logically isolate faults.
- 1.4 Troubleshooting Wideband Electrical Card(WBE-28 and WBE-84 Cards) FEAC on DS3 Ports
- 1.5 Troubleshooting WBE-28 and WBE-84 Cards with Far End Loopcodes on DS1 Ports
- 1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks—Explains how to perform loopback tests for CE100T-8 ports (and intermediate node OC-N ports the Ethernet circuit is mapped through). Follow these instructions to test an Ethernet circuit through the network or logically isolate faults.
- 1.7 Verify Wiring from the ONS 15310-MA Shelf and DSX Wiring Panel—Explains how to use the ONS 15310-MA DSX Wiring Verification Kit to test the DS-1 and DS-3 wiring between an ONS 15310-MA shelf and the digital signal cross-connect (DSX) wiring panel.

The remaining sections describe symptoms, problems, and solutions that are categorized according to the following topics:

- 1.8 Restore the Database and Default Settings—Explains how to restore software data and restore the node to the default setup.
- 1.9 PC Connectivity Troubleshooting—Provides troubleshooting procedures for Microsoft Microsoft Windows PC and network connectivity to the ONS 15310-CL or ONS 15310-MA.
- 1.10 CTC Operation Troubleshooting—Provides troubleshooting procedures for Cisco Transport Controller (CTC) login or operation problems.
- 1.11 Circuits and Timing—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.
- 1.12 Fiber and Cabling—Provides troubleshooting procedures for fiber and cabling connectivity errors.
- 1.13 Power and LED Tests—Provides troubleshooting procedures for power problems and lists LED behavior.

1.1 Network Troubleshooting Tests

Use loopbacks and hairpins to test newly created circuits before running live traffic or to logically locate the source of a network failure. Both the ONS 15310-CL and ONS 15310-MA allow electrical, optical, and Ethernet loopbacks:

- For the ONS 15310-CL, the 15310-CL-CTX controller card contains DS-1, DS-3, EC-1, and OC-3 or OC-12 optical ports which can be loopbacked. The CE-100T-8 Ethernet cards can be loopbacked, but the ML-100T-8 Ethernet card cannot support this function.
- For the ONS 15310-MA, the CTX2500 card controller card contains OC-N ports that can support optical loopbacks. The DS1-28/DS3-EC1-3 card and DS1-84/DS3-EC1-3 card support electrical loopbacks. The CE-100T-8 Ethernet card supports loopbacks, but the ML-100T-8 card does not.

1.1.1 Facility Loopback

A facility loopback tests a card's line interface unit (LIU) and related cabling. After applying a facility loopback on a port, use an optical or electrical test set, as appropriate, to run traffic over the loopback. A successful facility loopback isolates the card LIU or the cabling plant as the potential cause of a network problem.

Caution Before performing a facility loopback on any port, make sure there are at least two data communications channel (DCC) paths to the node where the card is installed. A second DCC provides a nonlooped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the node containing the loopback port.

Caution A facility loopback applies to an entire facility and not to an individual circuit. Exercise caution when using loopbacks on an OC-N port carrying live traffic because this traffic can be interrupted.

Note In CTC, the facility loopback is sometimes called a "facility (line)" loopback to indicate the direction that the loopback signal travels, that is, toward the span.

1.1.2 Terminal Loopback

A terminal loopback tests a circuit path as it passes through the cross-connect pathways of the node and loops back from the port where the loopback originates. A terminal loopback on an OC-N port turns the signal around before it reaches the LIU and sends it back through the card. This test verifies that the card's cross-connect circuit paths are valid.

For example, if you place a terminal loopback on a ONS 15310-CL optical port, the test-set traffic enters on the 15310-CL-CTX DS-3 port and travels toward the OC-N port. The terminal loopback placed on this OC-N port turns the signal around before it reaches the LIU, sending it back through the card to the electrical port. This test verifies that the optical cross-connect paths are valid (but it does not test the LIU for the OC-N port).

Note In CTC, the terminal loopback is sometimes called a "terminal (inward)" loopback, indicating the direction that the loopback signal travels—that is, back toward the port where it originated.

Note Due to hardware limitations on a terminal loopback, you cannot send an AIS downstream on a Cisco ONS 15310-CL CTX card.

1.1.3 Hairpin Circuit

A hairpin circuit brings traffic in and out on an electrical port instead of sending the traffic onto the OC-N line. A hairpin loops back only one specific synchronous transport signal (STS) or virtual tributary (VT) circuit. This kind of circuit test can be run on a node running live traffic because it does not affect the rest of the facility's traffic.

1.1.4 Cross-Connect Loopback

A cross-connect loopback tests a circuit path as it passes through the cross-connect portion of the 15310-CL-CTX or CTX2500 card and loops back to the port being tested. Testing and verifying circuit integrity often involves taking down the whole line; however, a cross-connect loopback allows you to create a loopback on any embedded channel at supported payloads at the STS-1 granularity and higher. For example, you can loop back a single STS-1 on an optical facility without interrupting the other STS circuits.

You can create a cross-connect loopback on working or protect OC-3 optical ports unless the protect port is used in a 1+1 protection group and is in working mode.

Note If a terminal or facility loopback exists on an optical port, you cannot use the cross-connect loopback.

1.2 Identify Points of Failure on an Electrical Circuit Path

Facility loopbacks, hairpin circuits, and terminal loopbacks are often used to test a circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure.

The tests in this section can be used to test DS-1, DS-3, or EC-1 circuits on a path protection configuration. Using a series of facility loopbacks, hairpin circuits, and terminal loopbacks, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of network test procedures applies to this scenario:

1. Facility loopback on the source-node port
2. Hairpin on the source-node port
3. Terminal loopback to the destination-node port
4. Hairpin on the destination-node port
5. Facility loopback to the destination-node port

Note The test sequence for your circuits differs according to the type of circuit and network topology.

Note Facility and terminal loopback tests require on-site personnel.

Note These procedures are performed when power connections to the nodes or sites are within necessary specifications. If the network tests do not isolate the problems, troubleshoot outward for power failure.

1.2.1 Perform a Facility Loopback on a Source-Node Port

The facility loopback test is performed on the node source port in the network circuit. Completing a successful facility loopback on this port isolates the cabling and port as possible failure points.

Caution Performing a loopback on an in-service circuit is service-affecting.

Note Loopbacks operate only on ports in the Out-of-Service, Maintenance (OOS,MT) administrative state and Out-of-Service and Management, Maintenance (OOS-MA,MT) service state. Brief instructions are given in each procedure for changing the port's state. For more information about port state, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Create the Facility Loopback on the Source-Node Port

Step 1 Connect an electrical test set to the DS-1, DS-3, or EC-1 port you are testing. For the ONS 15310-CL, this port is located on the 15310-CL-CTX. For the ONS 15310-MA, this port is located on the DS1-28/DS3-EC1-3 or DS1-84/DS3-EC1-3.

Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the electrical test set to the port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to create the facility loopback on the port being tested:

a. In node view, double-click the card where you are performing the loopback, then click the appropriate tab:
   - **Maintenance > DS1 > Loopback**
   - **Maintenance > DS3 > Loopback**
   - **Maintenance > EC1 > Loopback**

b. Choose **OOS,MT** from the Admin State column for the port being tested.

c. Choose **Facility** from the Loopback Type column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Note It is normal for a facility loopback 2.7.160 LPBKFACILITY (DS1, DS3) or 2.7.161 LPBKFACILITY (EC1) condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 4 Continue with the "Test the Facility Loopback" procedure on page 1-5.

Test the Facility Loopback

Step 1 If the test set is not already sending traffic, send test-set traffic on the loopback circuit.

Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, complete the following steps:

a. Double-click the electrical card, then click the appropriate tab:
   - **Maintenance > DS1 > Loopback**
   - **Maintenance > DS3 > Loopback**
   - **Maintenance > EC1 > Loopback**

b. Choose None from the Loopback Type column for the port being tested.

c. Choose the appropriate state (**IS,AINS**; **OOS,DSBLD**; or **OOS,MT**) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty card, faulty port, or faulty cabling from the electrical port. Continue with the "Test the Electrical Cabling" procedure on page 1-6.

Test the Electrical Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the electrical port) with a cable known to be good.

If a cable known to be good is not available, test the suspect cable with a test set. Remove the suspect cable from the electrical port and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or suspect.

Step 2 Resend test-set traffic on the loopback circuit with a good cable installed.

Step 3 If the test set indicates a good circuit, the problem is probably the defective cable. Replace the defective cable, then clear the loopback:

a. Double-click the card, then click the appropriate tab:

- **Maintenance > DS1 > Loopback**
- **Maintenance > DS3 > Loopback**
- **Maintenance > EC1 > Loopback**

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state (**IS,AINS**; **OOS,DSBLD**; or **OOS,MT**) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty port. Continue with the "1.2.2 Perform a Hairpin on a Source-Node Port" procedure on page 1-6.

1.2.2 Perform a Hairpin on a Source-Node Port

The hairpin test is performed on the first port in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through this port isolates the possibility that the source port is the cause of the faulty circuit.

Create the Hairpin on the Source-Node Port

Step 1 Connect an electrical test set to the port you are testing.

- If you just completed the "1.2.1 Perform a Facility Loopback on a Source-Node Port" procedure on page 1-4, leave the electrical test set connected to the electrical port.
- If you are starting the current procedure without the electrical test set connected to the electrical port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the electrical connectors for the port you are testing.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the hairpin on the port being tested:

a. Click the **Circuits** tab and click **Create**.

b. Give the circuit an easily identifiable name, such as Hairpin1.

c. Set the circuit Type and Size to the normal preferences, such as STS and STS1.

d. Uncheck the Bidirectional check box and click **Next**.

e. In the Circuit Source dialog box, select the same Node, Slot, Port, and Type where the test set is connected and click **Next**.

f. In the Circuit Destination dialog box, use the same Node, Slot, Port, and Type used for the Circuit Source dialog box and click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a one-way circuit.

Step 5 Continue with the "Test the Hairpin Circuit" procedure on page 1-7.

Test the Hairpin Circuit

Step 1 If the test set is not already sending traffic, send test-set traffic on the loopback circuit.

Step 2 Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the hairpin loopback circuit. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Step 4 If the test set indicates a faulty circuit, there might be a problem with the port. Continue with the "1.2.3 Perform a Terminal Loopback on a Destination-Node Port" procedure on page 1-7.

1.2.3 Perform a Terminal Loopback on a Destination-Node Port

The terminal loopback test is performed on the node destination port in the circuit. First, create a bidirectional circuit that originates on the source node electrical port (such as DS-1, DS-3, or EC-1) and terminates on the destination-node electrical port. Then continue with the terminal loopback test. Completing a successful terminal loopback to a destination-node port verifies that the circuit is good up to the destination port.

Caution Performing a loopback on an in-service circuit is service-affecting.

Create the Terminal Loopback on a Destination-Node Port

Step 1 Connect an electrical test set to the port you are testing:

a. If you just completed the "1.2.2 Perform a Hairpin on a Source-Node Port" procedure on page 1-6, leave the electrical test set connected to the electrical port in the source node.

b. If you are starting the current procedure without the electrical test set connected to the port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the connectors for the electrical port you are testing.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the terminal loopback circuit on the port being tested:

a. Click the **Circuits** tab and click **Create**.

b. Give the circuit an easily identifiable name, such as DSNtoDSN.

c. Set circuit Type and Size to the normal preferences, such as STS and STS1.

d. Leave the Bidirectional check box checked and click **Next**.

e. In the Circuit Source dialog box, fill in the source Node, Slot, Port, and Type where the test set is connected and click **Next**.

f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the electrical port in the destination node) and click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note Loopbacks operate only on ports in the OOS,MT administrative state.

Note It is normal for a 2.7.164 LPBKTERMINAL (DS1, DS3) or 2.7.165 LPBKTERMINAL (EC1) condition to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal loopback on the destination port being tested:

a. Go to the node view of the destination node:

- From the **View** menu, choose **Go To Other Node**.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the destination node (ONS 15310-CL or ONS 15310-MA).

c. Double-click the correct card, then click the appropriate following tabs:

- **Maintenance > DS1 > Loopback**
- **Maintenance > DS3 > Loopback**
- **Maintenance > EC1 > Loopback**

d. Select **OOS,MT** from the Admin State column.

e. Select **Terminal** from the Loopback Type column.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

Step 6 Continue with the "Test the Terminal Loopback Circuit on the Destination-Node Port" procedure on page 1-9.

Test the Terminal Loopback Circuit on the Destination-Node Port

Step 1 If the test set is not already sending traffic, send test-set traffic on the loopback circuit.

Step 2 Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the terminal loopback:

a. Double-click the 15310-CL-CTX or CTX2500 card in the destination node with the terminal loopback.

b. Double-click the appropriate card containing the electrical circuit you are testing, and click the appropriate tab:

- **Maintenance > DS1 > Loopback**
- **Maintenance > DS3 > Loopback**
- **Maintenance > EC1 > Loopback**

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (IS,AINS,AINS OOS,DSBLD or OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty port. Continue with the "1.2.5 Perform a Hairpin Test on a Destination-Node Port" procedure on page 1-13.

1.2.4 Perform a Network Interface Unit Loopback on a Destination-Node Port

The network interface unit (NIU) loopback test is performed on the node destination port in the circuit. First, create a bidirectional circuit that originates on the source node electrical port (DS-1) and terminates on the destination-node electrical port. Then continue with the NIU loopback test. Completing a successful NIU loopback to a destination-node port verifies that the circuit is good up to the destination port.

Note NIU loopback is applicable for ESF frame format only.

Caution Performing a loopback on an in-service circuit is service-affecting.

DS1 Inhibit FEAC Backplane Loopback

DS1 ports initiate loopbacks when they receive FEAC loop codes. If the Inhibit FE Backplane Lbk check box is checked for a DS1 port, that port ignores any FEAC loop codes it receives and will not loop back (return them).

Create the NIU Loopback on a Destination-Node DS1 Port

Step 1 Connect a test set to the near end DS1 port.

Note For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

If you are starting the current procedure without the test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the test set to the port you are testing. Both Tx and Rx connect to the same port.

Step 2 Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Step 3 Use CTC to set up the terminal loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as VT, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as C1C1toC1C6.

e. Leave the Bidirectional check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and DS1 where the test set is connected as shown in Figure 1-2.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, select the Node, card Slot, Port, and DS1 connected to CPE as shown in Figure 1-2.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Step 5 Create NIU Loopback on the destination port being tested:

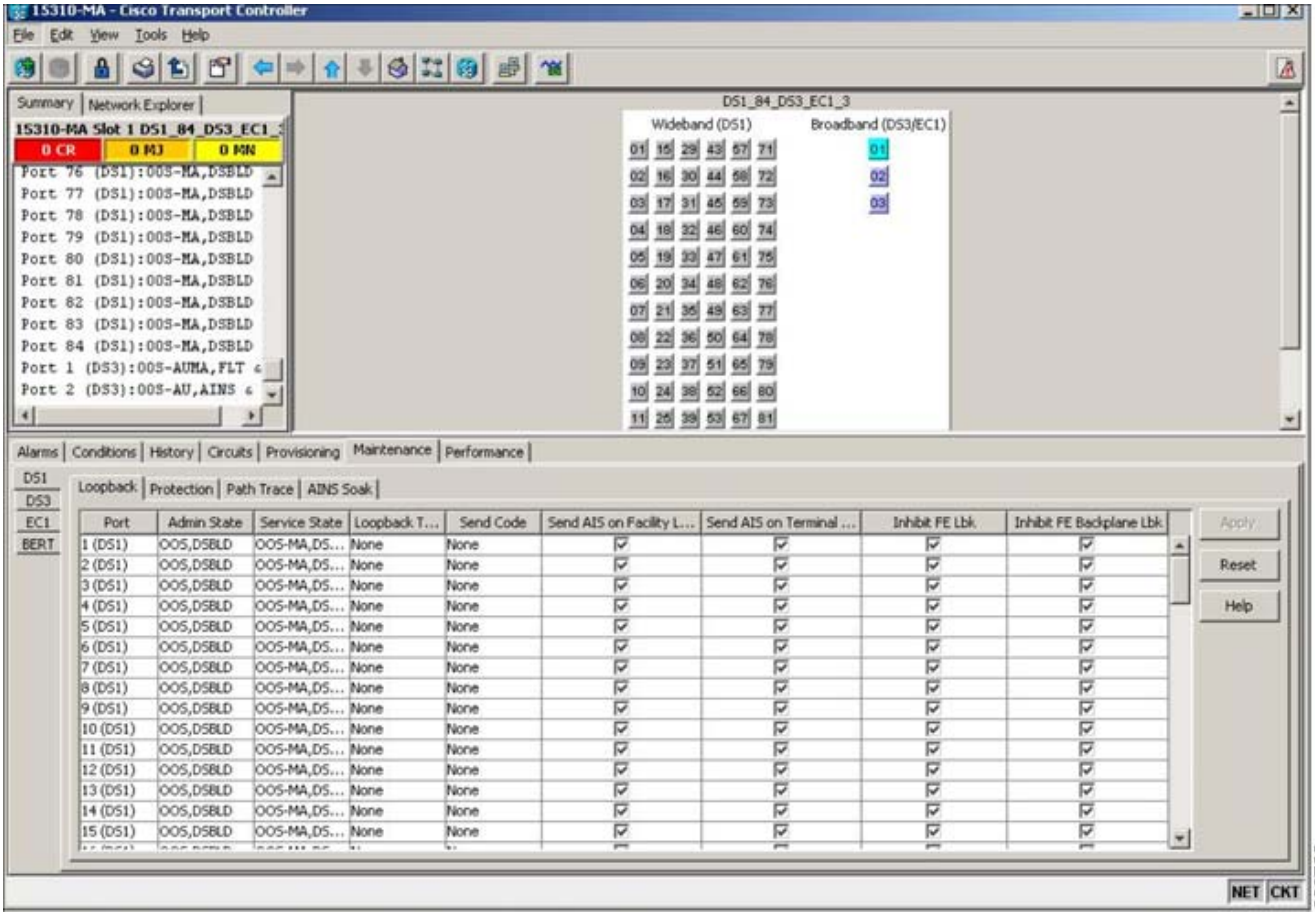
a. Go to the card view of the destination node:

b. Click the **Maintenance > DS1 > Loopback** tabs.

c. Uncheck the Inhibit FE Backplane Lbk checkbox for port being tested.

Note The Inhibit FE Backplane Lbk checkbox is always checked by default.

Figure 1-1 Accessing FEAC Functions on the DS1 ports of WBE-28/WBE-84 Cards



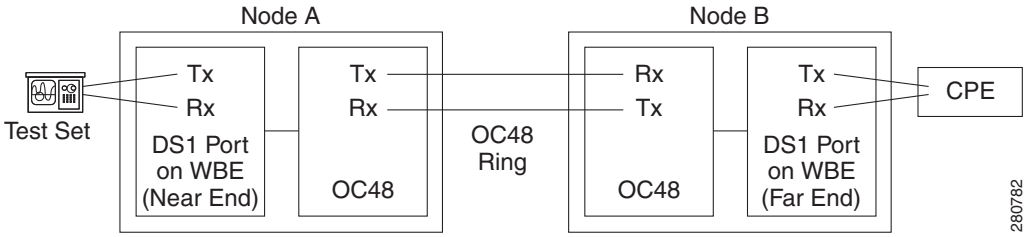
d. Click **Apply**.

Step 6 Send activate loop codes from the test set.

The destination port senses the loop codes form the test set and creates NIU terminal loopback on that port.

Note It is normal for a 2.7.164 LPBKTERMINAL (DS1, DS3) condition to appear during a loopback setup. The condition clears when you remove the loopback.

Figure 1-2 Diagram of FEAC Circuit



Step 7 Complete the "Test and Clear the DS1 NIU Loopback Circuit" procedure.

Test and Clear the DS1 NIU Loopback Circuit

Step 1 If the test set is not already sending traffic, send test-set traffic on the loopback circuit.

Step 2 Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the NIU loopback through the test set or through CTC:

Step 4 Clear NIU loopback from the test set by sending the deactivate loop codes.

Clear NIU loopback through CTC:

a. Double-click the destination node DS1 card with the NIU loopback.

b. Click the **Maintenance** > **DS1** > **Loopback** tabs:

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 5 Clear the NIU loopback circuit:

a. Click the **Circuits** tab.

b. Choose the NIU loopback circuit being tested.

c. Click **Delete**.

Note If you delete the NIU loopback circuit without clearing the NIU loopback (Step 4), you have to manually clear the NIU loopback through the test set or CTC.

d. Click **Yes** in the Delete Circuits dialog box.

The entire circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

Note If the destination port needs to be reused for other purposes, enable the Inhibit FE Backplane Lbk checkbox.

a. Go to the card view of the destination node:

b. Click the **Maintenance** > **DS1** > **Loopback** tabs.

c. Enable the Inhibit FE Backplane Lbk checkbox for port being tested.

d. Click **Apply**.

1.2.5 Perform a Hairpin Test on a Destination-Node Port

The hairpin test is performed on the port in the destination node. To perform this test, you must also create a bidirectional circuit in the transmit direction from the destination ONS 15310-CL or ONS 15310-MA to the source node. Creating the bidirectional circuit and completing a successful hairpin eliminates the possibility that the source port, destination port, or fiber span is responsible for the faulty circuit.

Create the Hairpin Loopback Circuit on the Destination-Node Port

Step 1 Connect an electrical test set to the electrical port you are testing.

Use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the electrical cabling panel for the port you are testing.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the source loopback circuit on the port being tested:

a. Click the **Circuits** tab and click **Create**.

b. Give the circuit an easily identifiable name, such as Hairpin1.

c. Set the circuit Type and Size to the normal preferences, such as STS and STS1.

d. Leave the Bidirectional check box checked and click **Next**.

e. In the Circuit Source dialog box, fill in the source Node, Slot, Port, and Type where the test set is connected and click **Next**.

f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the port in the destination node) and click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Step 5 Use CTC to set up the destination hairpin circuit on the port being tested.

Note The destination loopback circuit on a port is a one-way test.

For example, in a typical east-to-west slot configuration, a DS-3 port on the source node is one end of the fiber span, and a DS-3 port on the destination node is the other end.

a. Click the **Circuits** tab and click **Create**.

b. Give the circuit an easily identifiable name, such as Hairpin1.

c. Set the Circuit Type and Size to the normal preferences, such as STS and STS1.

d. Uncheck the Bidirectional check box and click **Next**.

e. In the Circuit Source dialog box, select the same Node, Slot, Port, and Type where the previous circuit is connected and click **Next**.

f. In the Circuit Destination dialog box, use the same Node, Slot, Port, and Type used for the Circuit Source dialog box and click **Finish**.

Step 6 Confirm that the newly created circuit appears on the Circuits tab list as a one-way circuit.

Step 7 Verify that the circuits connect to the correct slots. For example, verify that source node OC-N port (east slot) is connected to the destination node (west slot). If two east slots or two west slots are connected, the circuit does not work. Except for the distinct slots, all other circuit information, such as ports, should be identical.

Step 8 Continue with the "Test the Hairpin Circuit" procedure on page 1-14.

Test the Hairpin Circuit

Step 1 If the test set is not already sending traffic, send test-set traffic on the loopback circuit.

Step 2 Examine the test traffic received by the test set. Look for errors or any other signal information indicated by the test set.

Step 3 If the test set indicates a good circuit, no further testing is necessary; clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

f. Continue with the "1.2.6 Perform a Facility Loopback on a Destination Port" procedure on page 1-14.

1.2.6 Perform a Facility Loopback on a Destination Port

The final facility loopback test is performed on the last port in the circuit— in this case the port in the destination node. Completing a successful facility loopback on this port isolates the possibility that the destination-node cabling, card, or LIU is responsible for a faulty circuit.

Caution Performing a loopback on an in-service circuit is allowed but is service-affecting.

Note Loopbacks operate only on ports in the OOS,MT administrative state.

Create a Facility Loopback Circuit on a Destination Port

Step 1 Connect an electrical test set to the port you are testing:

a. If you just completed the "1.2.5 Perform a Hairpin Test on a Destination-Node Port" procedure on page 1-13, leave the electrical test set connected to the electrical port in the destination node.

b. If you are starting the current procedure without the electrical test set connected to the electrical port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the electrical interface panel.

c. Adjust the test set accordingly.

Step 2 Use CTC to create the facility loopback on the port being tested:

a. In node view, double-click the card where you are performing the loopback, then click the appropriate tab:
   - **Maintenance > DS1 > Loopback**
   - **Maintenance > DS3 > Loopback**
   - **Maintenance > EC1 > Loopback**

b. Select **Facility** from the Loopback Type column for the port being tested. If you are creating a loopback on a multiport card, select the row appropriate for the desired port.

c. Click **Apply**.

d. Click **Yes** in the confirmation dialog box.

Note It is normal for a 2.7.160 LPBKFACILITY (DS1, DS3) or 2.7.161 LPBKFACILITY (EC1) condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 3 Continue with the "Test the Facility Loopback Circuit" procedure on page 1-15.

Test the Facility Loopback Circuit

Step 1 If the test set is not already sending traffic, send test-set traffic on the loopback circuit.

Step 2 Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the loopback circuit.

a. Clear the facility loopback:

b. Double-click the card, then click the appropriate tab:
   - **Maintenance > DS1 > Loopback**
   - **Maintenance > DS3 > Loopback**
   - **Maintenance > EC1 > Loopback**

c. Choose **None** from the Loopback Type column for the port being tested.

d. Choose the appropriate state (**IS,AINS**; **OOS,DSBLD**; or **OOS,MT**) from the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

The entire electrical circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

Step 4 If the test set indicates a faulty circuit, the problem might be a faulty card or faulty cabling. Continue with the "Test the Electrical Cabling" procedure on page 1-16.

Test the Electrical Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the DS-1, DS-3, or EC-1 port) with a cable known to be good.

If a cable known to be good is not available, test the suspect cable with a test set. Remove the suspect cable from the electrical port and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or suspect.

Step 2 Resend test traffic on the loopback circuit with a good cable installed.

Step 3 If the test set indicates a good circuit, the problem is probably the defective cable. Replace the defective cable.

Step 4 Clear the facility loopback:

a. Double-click the card and then click the appropriate tab:
   - **Maintenance > DS1 > Loopback**
   - **Maintenance > DS3 > Loopback**
   - **Maintenance > EC1 > Loopback**

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state (**IS,AINS**; **OOS,DSBLD**; or **OOS,MT**) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

The entire DS-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

1.3 Identify Points of Failure on an OC-N Circuit Path

Using facility loopbacks, terminal loopbacks, and cross-connect loopback circuits, you can test OC-N facilities or STSs on the ONS 15310-CL or ONS 15310-MA to logically isolate faults. For this purpose, you perform a loopback test at each point along the circuit path to systematically isolate a point of failure.

The example in this section tests an OC-N circuit on a three-node path protection configuration. Using a series of facility loopbacks and terminal loopbacks, the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of seven network test procedures applies to this sample scenario:

1. Facility loopback on the source-node OC-N port
2. Cross-connect loopback on the source-node OC-N port
3. Terminal loopback on the source-node OC-N port
4. Facility loopback on the intermediate-node OC-N port
5. Terminal loopback on the intermediate-node OC-N port
6. Facility loopback on the destination-node OC-N port
7. Terminal loopback on the destination-node OC-N port

Note The test sequence for your circuits differs according to the type of circuit and network topology.

Note Facility and terminal loopback tests require on-site personnel.

1.3.1 Perform a Facility Loopback on a Source-Node OC-N Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the source 15310-CL-CTX or CTX2500 card OC-N port in the source node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point. Performing a loopback on an in-service circuit is service-affecting.

Create the Facility Loopback on the Source OC-N Port

Step 1 Connect an optical test set to the port you are testing.

Use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing.

Step 2 Use CTC to create the facility loopback circuit on the port being tested:

a. In node view, double-click the controller card (15310-CL-CTX or CTX2500) to display the card view.

b. Click the **Maintenance > Optical > Loopback > Port** tabs.

c. Choose **OOS,MT** from the Admin State column for the port being tested.

d. Choose **Facility** from the Loopback Type column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Note It is normal for a 2.7.162 LPBKFACILITY (OCN) condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 3 Continue with the "Test the Facility Loopback Circuit" procedure on page 1-17.

Test the Facility Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback:

g. Click the **Maintenance > Optical > Loopback > Port** tabs.

h. Choose **None** from the Loopback Type column for the port being tested.

i. Choose the appropriate state (**IS,AINS**; **OOS,DSBLD**; or **OOS,MT**) from the Admin State column for the port being tested.

j. Click **Apply**.

k. Click **Yes** in the confirmation dialog box.

l. Continue with the "1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port" procedure on page 1-18.

1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port

The cross-connect loopback test occurs on the cross-connect portion of the controller card (15310-CL-CTX or CTX2500 card) in a network circuit. Completing a successful cross-connect loopback through the card isolates the possibility that the cross-connect is the cause of the faulty circuit.

Create the Cross-Connect Loopback on the Source OC-N Port

Step 1 Connect an optical test set to the port you are testing:

a. If you just completed the "1.3.1 Perform a Facility Loopback on a Source-Node OC-N Port" procedure on page 1-17, leave the optical test set connected to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set connected to the OC-N port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing.

c. Adjust the test set accordingly.

Step 2 Use CTC to put the circuit being tested out of service:

a. In node view, click the **Circuits** tab.

b. Click the circuit and then click **Edit**.

c. In the Edit Circuit dialog box, click the **State** tab.

d. Choose **OOS-MT** from the Target Circuit Admin State drop-down list.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 3 Use CTC to set up the cross-connect loopback on the circuit being tested:

a. In node view, double-click the 15310-CL-CTX or CTX2500 to open the card view.

b. For the OC-N port, click the **Maintenance > Optical > Loopback > SONET STS** tabs.

c. Click the check box in the XC Loopback column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 4 Continue with the "Test the Cross-Connect Loopback Circuit" procedure on page 1-19.

Test the Cross-Connect Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the cross-connect. Clear the cross-connect loopback:

a. In card view, click the **Maintenance > Optical > Loopback > SONET STS** tabs.

b. Uncheck the check box in the XC Loopback column for the circuit being tested.

c. Click **Apply**.

d. Click **Yes** in the confirmation dialog box.

Step 4 If the test set indicates a faulty circuit, there might be a problem with the cross-connect portion of the 15310-CL-CTX or CTX2500 card. Complete the "1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port" procedure on page 1-19.

1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the source node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then continue with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N. Performing a loopback on an in-service circuit is service-affecting.

Create the Terminal Loopback on a Source Node OC-N Port

Step 1 Connect an optical test set to the port you are testing:

a. If you just completed the "1.3.2 Perform a Cross-Connect Loopback on the Source OC-N Port" procedure on page 1-18, leave the optical test set connected to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set connected to the OC-N port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal loopback circuit on the port being tested:

a. Click the **Circuits** tab and click **Create**.

b. Give the circuit an easily identifiable name, such as OCN1toOCN2.

c. Set circuit Type and Size to the normal preferences, such as STS and STS1.

d. Verify that Bidirectional is checked.

e. Click **Next**.

f. In the Circuit Source dialog box, fill in the same Node, Slot, Port, and Type where the test set is connected and click **Next**.

g. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the OC-N port in the source node) and click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for a 2.7.166 LPBKTERMINAL (OCN) condition to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the terminal loopback on the destination port being tested:

a. In node view, double-click the card that requires the loopback.

b. Click the **Maintenance > Optical > Loopback > Port** tabs.

c. Select **OOS,MT** from the Admin State column.

d. Select **Terminal** from the Loopback Type column.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 5 Continue with the "Test the Terminal Loopback Circuit" procedure on page 1-20.

Test the Terminal Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

If the test set indicates a good circuit, no further testing is necessary on the loopback circuit:

Step 3 Clear the terminal loopback:

a. Double-click the card in the source node having the terminal loopback.

b. Click the **Maintenance > Optical > Loopback > Port** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (**IS,AINS**; **OOS,DSBLD**; or **OOS,MT**) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty port. Continue with the "1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-21.

1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port

The facility loopback test is performed on the node source port in the network circuit, in this example, the source OC-N port in the intermediate node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point.

Caution Performing a loopback on an in-service circuit is service-affecting.

Create the Facility Loopback on an Intermediate-Node OC-N Port

Step 1 Connect an optical test set to the port you are testing:

a. If you just completed the "1.3.3 Perform a Terminal Loopback on a Source-Node OC-N Port" procedure on page 1-19, leave the optical test set connected to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set connected to the OC-N port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the facility loopback circuit on the port being tested:

a. Click the **Circuits** tab and click **Create**.

b. Give the circuit an easily identifiable name, such as OCN1toOCN3.

c. Set circuit Type and Size to the normal preferences, such as STS and STS1.

d. Verify that Bidirectional is checked and click **Next**.

e. In the Circuit Source dialog box, fill in the source Node, Slot, Port, and Type where the test set is connected and click **Next**.

f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the OC-N port in the intermediate node) and click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for a 2.7.162 LPBKFACILITY (OCN) condition to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the facility loopback on the destination port being tested:

a. Go to the node view of the intermediate node:

- From the **View** menu, choose **Go To Other Node**.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the controller card (15310-CL-CTX or CTX2500) in the intermediate node.

c. Click the **Maintenance > Optical > Loopback > Port** tabs.

d. Select **OOS,MT** from the Admin State column.

e. Select **Facility** from the Loopback Type column.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

Note It is normal for a 2.7.162 LPBKFACILITY (OCN) condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 5 Continue with the "Test the Facility Loopback Circuit" procedure on page 1-22.

Test the Facility Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

If the test set indicates a good circuit, no further testing is necessary with the facility loopback:

Step 3 Clear the facility loopback:

a. Click the **Maintenance > Optical > Loopback > Port** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state (**IS,AINS**; **OOS,DSBLD**; or **OOS,MT**) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 4 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty OC-N port. Continue with the "1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port" procedure on page 1-22.

1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port

The terminal loopback test is performed on the node destination port in the circuit, in this example, the destination OC-N port in the intermediate node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then continue with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N port.

Caution Performing a loopback on an in-service circuit is service-affecting.

Create the Terminal Loopback on an Intermediate-Node OC-N Port

Step 1 Connect an optical test set to the port you are testing:

a. If you just completed the "1.3.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-21, leave the optical test set connected to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set connected to the OC-N port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal loopback circuit on the port being tested:

a. Click the **Circuits** tab and click **Create**.

b. Give the circuit an easily identifiable name, such as OCN1toOCN4.

c. Set circuit Type and Size to the normal preferences, such as STS and STS1.

d. Leave the Bidirectional check box checked and click **Next**.

e. In the Circuit Source dialog box, fill in the source Node, Slot, Port, and Type where the test set is connected and click **Next**.

f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the OC-N port in the intermediate node) and click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for a 2.7.166 LPBKTERMINAL (OCN) condition to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the terminal loopback on the destination port being tested:

a. Go to the node view of the intermediate node:

- From the **View** menu, choose **Go To Other Node**.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the controller card (15310-CL-CTX or CTX2500) with the OC-N port requiring a loopback.

c. Click the **Maintenance > Optical > Loopback > Port** tabs.

d. Select **OOS,MT** from the Admin State column.

e. Select **Terminal** from the Loopback Type column.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

Step 5 Continue with the "Test the Terminal Loopback Circuit" procedure on page 1-24.

Test the Terminal Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

If the test set indicates a good circuit, no further testing is necessary on the loopback circuit.

Step 3 Clear the terminal loopback:

a. Double-click the card with the loopback.

b. Click the **Maintenance > Optical > Loopback > Port** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (**IS,AINS**; **OOS,DSBLD**; or **OOS,MT**) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty controller card (15310-CL-CTX or CTX2500). Continue with the "1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port" procedure on page 1-24.

1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port

The final facility loopback test is performed on the source OC-N port in the destination node. Completing a successful facility loopback on this port isolates the OC-N port as a possible failure point.

Caution Performing a loopback on an in-service circuit is service-affecting.

Create the Facility Loopback on a Destination-Node OC-N Port

Step 1 Connect an optical test set to the port you are testing:

a. If you just completed the "1.3.5 Perform a Terminal Loopback on an Intermediate-Node OC-N Port" procedure on page 1-22, leave the optical test set connected to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set connected to the OC-N port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the facility loopback circuit on the port being tested:

a. Click the **Circuits** tab and click **Create**.

b. Give the circuit an easily identifiable name, such as OCN1toOCN5.

c. Set circuit Type and Size to the normal preferences, such as STS and STS1.

d. Leave the Bidirectional check box checked and click **Next**.

e. In the Circuit Source dialog box, fill in the source Node, Slot, Port, and Type where the test set is connected and click **Next**.

f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the OC-N port in the destination node) and click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for a 2.7.162 LPBKFACILITY (OCN) condition to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the facility loopback on the destination port being tested:

a. Go to the node view of the destination node:

- From the **View** menu, choose **Go To Other Node**.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the 15310-CL-CTX or CTX2500 card with the OC-N port that requires the loopback.

c. Click the **Maintenance > Optical > Loopback > Port** tabs.

d. Select **OOS,MT** from the Admin State column.

e. Select **Terminal** from the Loopback Type column.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

Note It is normal for a 2.7.162 LPBKFACILITY (OCN) condition to appear during loopback setup. The condition clears when you remove the loopback.

Step 5 Continue with the "Test the Facility Loopback Circuit" procedure on page 1-25.

Test the Facility Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

If the test set indicates a good circuit, no further testing is necessary with the facility loopback:

Step 3 Clear the facility loopback:

a. Click the **Maintenance > Optical > Loopback > Port** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state (IS,AINS; OOS,DSBLD; or OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 4 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box.

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty OC-N port. Continue with the "1.3.7 Perform a Terminal Loopback on a Destination-Node OC-N Port" procedure on page 1-26.

1.3.7 Perform a Terminal Loopback on a Destination-Node OC-N Port

The terminal loopback test is performed on the destination OC-N port in the destination node. First, create a bidirectional circuit that starts on the node source OC-N port and loops back on the node destination OC-N port. Then continue with the terminal loopback test. Completing a successful terminal loopback to a node destination OC-N port verifies that the circuit is good up to the destination OC-N.

Caution Performing a loopback on an in-service circuit is service-affecting.

Create the Terminal Loopback on a Destination-Node OC-N Port

Step 1 Connect an optical test set to the port you are testing:

a. If you just completed the "1.3.6 Perform a Facility Loopback on a Destination-Node OC-N Port" procedure on page 1-24, leave the optical test set connected to the OC-N port in the source node.

b. If you are starting the current procedure without the optical test set connected to the OC-N port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing.

c. Adjust the test set accordingly.

Step 2 Use CTC to set up the terminal loopback circuit on the port being tested:

a. Click the **Circuits** tab and click **Create**.

b. Give the circuit an easily identifiable name, such as OCN1toOCN6.

c. Set circuit Type and Size to the normal preferences, such as STS and STS1.

d. Leave the Bidirectional check box checked and click **Next**.

e. In the Circuit Source dialog box, fill in the source Node, Slot, Port, and Type where the test set is connected and click **Next**.

f. In the Circuit Destination dialog box, fill in the destination Node, Slot, Port, and Type (the OC-N port in the destination node) and click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for a 2.7.166 LPBKTERMINAL (OCN) condition to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the terminal loopback on the destination port being tested:

a. Go to the node view of the destination node:
- From the **View** menu, choose **Go To Other Node**.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the controller card (15310-CL-CTX or CTX2500) with the OC-N port that requires the loopback, such as the 15310-CL-CTX in the destination-node ONS 15310-CL.

c. Click the **Maintenance > Optical > Loopback > Port** tabs.

d. Select **OOS,MT** from the Admin State column.

e. Select **Terminal** from the Loopback Type column.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

Step 5 Continue with the "Test the Terminal Loopback Circuit" procedure on page 1-27.

Test the Terminal Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit:

a. Clear the terminal loopback:
- Double-click the card terminal node with the terminal loopback.
- Click the **Maintenance > Optical > Loopback > Port** tabs.
- Select **None** from the Loopback Type column for the port being tested.
- Select the appropriate state (**IS,AINS**; **OOS,DSBLD**; or **OOS,MT**) in the Admin State column for the port being tested.
- Click **Apply**.
- Click **Yes** in the confirmation dialog box.

b. Clear the terminal loopback circuit:
- Click the **Circuits** tab.
- Choose the loopback circuit being tested.

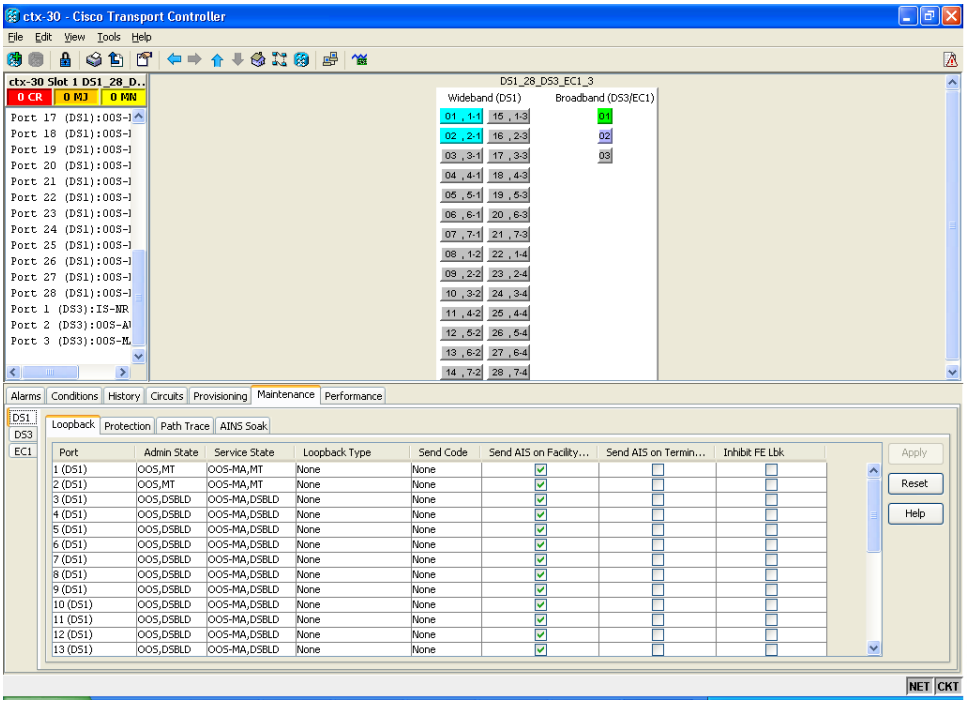
- Click **Delete**.
- Click **Yes** in the Delete Circuits dialog box.

If no fault is found, the entire OC-N circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

1.4 Troubleshooting Wideband Electrical Card(WBE-28 and WBE-84 Cards) FEAC on DS3 Ports

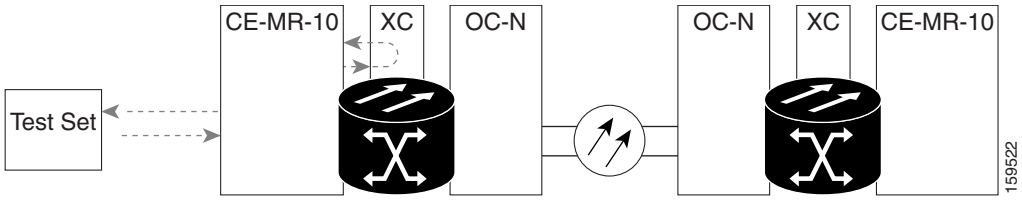
WBE-28/WBE-84 cards support far-end alarm and control(FEAC) functions on DS3 ports. Click the WBE-28/WBE-84 **Maintenance > DS3** tabs at the card view to reveal the two additional function columns. Figure 1-1 shows the DS3 subtab and the additional Send Code and Inhibit FE Lbk function columns.

Figure 1-3 Accessing FEAC Functions on the DS3 ports of WBE-28/WBE-84 Cards



The "far end" in FEAC refers to the equipment connected to the WBE card and not to the far end of a circuit. In Figure 1-2, if a WBE-28/WBE-84 DS3 (near-end) port is configured to send a line loop code, the code will be sent to the connected test set, not the WBE-28/WBE-84 DS3 (far-end) port. FEAC functions will be available only when the DS3 port is configured in CBIT Framing.

Figure 1-4 Diagram of FEAC Circuit



1.4.1 FEAC Send Code

The Send Code column on the WBE-28/WBE-84 cards Maintenance tab only applies to OOS-MA,MT ports configured for CBIT framing. The column lets a user select No Code (the default) or line loop code. Selecting line loop code inserts a line loop activate FEAC in the CBIT overhead transmitting to the connected facility. This code initiates a loopback from the facility to the ONS 15310-MA. Selecting No Code sends a line-loop-deactivate FEAC code to the connected equipment, which will remove the loopback.

1.4.2 WBE-28/WBE-84 Inhibit FEAC Loopback

WBE-28/WBE-84 DS3 ports initiate loopbacks when they receive FEAC line loop codes. If the Inhibit FE Lbk check box is checked for a DS3 port, that port ignores any FEAC line loop codes it receives and will not loop back (return them). If you inhibit a DS3 port's far end loopback response, this DS3 port is not restricted from terminal or facility loopbacks.

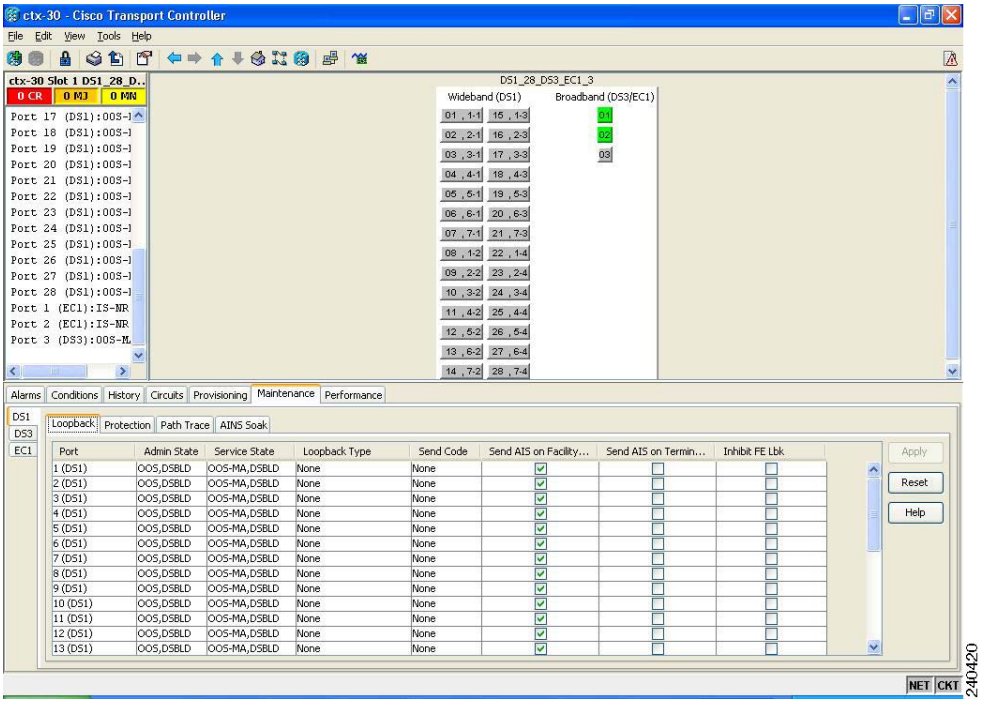
1.4.3 FEAC Alarms

When an ONS 15310MA - WBE-28/WBE-84 DS3 port receives an activation code for a FEAC loopback, it raises the "LPBKDS3FEAC" condition on page 2-108. The condition clears when the port receives the command to deactivate the FEAC loopback. If a node sends a FEAC loopback command to the far end, the sending node raises a "LPBKDS3FEAC-CMD" condition on page 2-109 for the near-end port.

1.5 Troubleshooting WBE-28 and WBE-84 Cards with Far End Loopcodes on DS1 Ports

WBE Cards support Far End Loopcodes when the DS1 port is operating in ESF Framing mode. Click the WBE-28/WBE-84 **Maintenance->DS1** tab to reveal additional columns, namely , "Inhibit FE Lbk" and "Send Code". Here we are using the term FE Loopcodes instead of FEAC in DS1, since DS1 supports only Far End Loopcodes, but NOT Alarms.

Figure 1-5 Accessing Far End troubleshooting Functions on the WBE Cards



Note The term "Far End" refers to the equipment connected to the WBE card and not to the far end of a circuit.

1.5.1 FEAC Send Code

The Send Code column on the WBE-28/WBE-84 card Maintenance tab only applies to OOS-MA,MT ports configured for ESF framing. The column lets a user select No Code (the default) or line loop code. Selecting line loop code inserts a line loop activate Far End Loopcode in the ESF overhead transmitting to the connected facility. This code initiates a loopback from the facility to the ONS 15454. Selecting No Code sends a line-loop-deactivate Far End Loopcode to the connected equipment, which will remove the loopback.

1.5.2 WBE-28/WBE-84 Inhibit FEAC Loopback

WBE-28/WBE-84 DS1 ports initiate loopbacks when they receive Far End line loop codes. If the Inhibit FE Lbk check box is checked for a DS1 port, that port ignores any Far End line loop codes it receives and will not loop back. If you inhibit a DS1 port's far end loopback response, this DS1 port is not restricted from terminal or facility loopbacks.

1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks

Facility loopbacks, terminal loopbacks, and cross-connect loopback circuits are often used together to test the circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure.

When performing this testing on networks that contain intermediate nodes, you will test the OC-N connection at intermediate nodes rather than CE100T-8 card connections. (The CE100T-8 is a mapper card and is only capable of supporting point-to-point circuits.)

You can use these procedures on CE100T-8 cards but not on ML-100T-8 Ethernet cards. Using a series of facility loopbacks and terminal loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains six network test procedures:

Note The test sequence for your circuits will differ according to the type of circuit and network topology.

1. A facility loopback on the source-node Ethernet port
2. A terminal loopback on the source-node Ethernet port
3. A facility loopback on the intermediate-node OC-N port
4. A terminal loopback on the intermediate-node OC-N port
5. A facility loopback on the destination-node Ethernet port
6. A terminal loopback on the destination-node Ethernet port

Note Facility and terminal loopback tests require on-site personnel.

1.6.1 Perform a Facility Loopback on a Source-Node Ethernet Port

The facility loopback test is performed on the node source port in the network circuit. Completing a successful facility loopback on this port isolates the port as a possible failure point.

Note Facility loopbacks require on-site personnel.

Caution Performing a loopback on an in-service circuit is service-affecting.

Complete the "Create the Facility Loopback on the Source-Node Ethernet Port" procedure on page 1-31.

Create the Facility Loopback on the Source-Node Ethernet Port

Step 1 Connect a test set to the port you are testing.

Note For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

Use appropriate cabling to attach the Tx and Rx terminals of the test set to the port you are testing. The Tx and Rx terminals connect to the same port.

Step 2 Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Step 3 In CTC node view, double-click the CE100T-8 card to display the card view.

Step 4 Click the **Maintenance > Loopback** tabs.

Step 5 Choose **OOS,MT** from the Admin State column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

Step 6 Choose **Facility** from the Loopback Type column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

Step 7 Click **Apply**.

Step 8 Click **Yes** in the confirmation dialog box.

Note It is normal for the "LPKTERMINAL (CE100T, CEMR)" condition on page 2-111 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the "Test and Clear the Facility Loopback Circuit" procedure on page 1-32.

Test and Clear the Facility Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback:

- **a.** Double-click the CE100T-8 card, then click the **Maintenance > Loopback** tabs.
- **b.** Choose **None** from the Loopback Type column for the port being tested.
- **c.** Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.
- **d.** Click **Apply**.
- **e.** Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Test the Ethernet Card" procedure on page 1-32.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-163 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card installed.

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the Return Materials Authorization (RMA) process. Contact Cisco Technical Support (1-800-553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-163 for the faulty card.

Step 5 Clear the facility loopback:

a. Double-click the CE100T-8 card, then click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "1.6.2 Perform a Terminal Loopback on a Source-Node Ethernet Port" procedure on page 1-33.

1.6.2 Perform a Terminal Loopback on a Source-Node Ethernet Port

The terminal loopback test is performed on the node source Ethernet port. To do this, you create a bidirectional circuit that starts on the node destination CE100T-8 port and loops back on node source CE100T-8 port. You then proceed with the terminal loopback test. Completing a successful terminal loopback to a node source port verifies that the circuit is good to the source port.

Note Terminal loopbacks require on-site personnel.

Caution Performing a loopback on an in-service circuit is service-affecting.

Complete the "Create the Terminal Loopback on a Source-Node Ethernet Port" procedure on page 1-33.

Create the Terminal Loopback on a Source-Node Ethernet Port

Step 1 Connect a test set to the port you are testing:

Note For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

a. If you just completed the "1.6.1 Perform a Facility Loopback on a Source-Node Ethernet Port" procedure on page 1-31, leave the test set hooked up to the Ethernet port in the source node.

b. If you are starting the current procedure without the test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the test set to the port you are testing. Both Tx and Rx connect to the same port.

Step 2 Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Step 3 Use CTC to set up the terminal loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as C1C1toC1C2.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPKTERMINAL (CE100T, CEMR)" condition on page 2-111 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal loopback on the destination port being tested:

a. In node view, double-click the card that requires the loopback, such as the destination G-Series card in the source node.

b. Click the **Maintenance > Loopback** tabs.

c. Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

d. Select **Terminal** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Test and Clear the Ethernet Terminal Loopback Circuit" procedure on page 1-35.

Test and Clear the Ethernet Terminal Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the terminal loopback state on the port:

a. Double-click the CE100T-8 card in the source node with the terminal loopback.

b. Click the **Maintenance > Loopback** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-35.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-163 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card.

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1-800-553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-163 for the defective card.

Step 5 Clear the terminal loopback on the port before testing the next segment of the network circuit path:

a. Double-click the CE100T-8 card with the terminal loopback in the source node.

b. Click the **Maintenance > Loopback** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 6 Clear the terminal loopback circuit before testing the next segment of the network circuit path:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

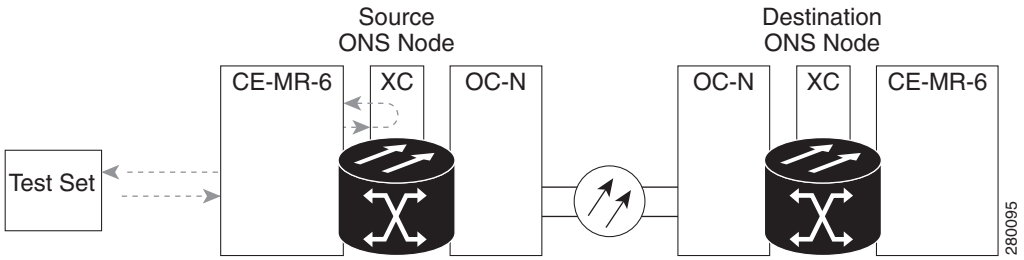
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.6.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-39.

1.6.3 Perform a Hairpin Test on a Source-Node Ethernet Port

The hairpin test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Figure 1-6 shows an example of a hairpin loopback on a source-node port.

Figure 1-6 Hairpin Loopback on a Source-Node Ethernet Port



Note The ONS 15310 does not support simplex operation on the cross-connect card. Two cross-connect cards of the same type must be installed for each node.

Note Hairpin loopbacks require on-site personnel.

Complete the "Create the Hairpin Circuit on the Source-Node Ethernet Port" procedure on page 1-37.

Create the Hairpin Circuit on the Source-Node Ethernet Port

Step 1 Connect an Ethernet test set to the port you are testing:

a. If you just completed the "1.6.2 Perform a Terminal Loopback on a Source-Node Ethernet Port" procedure on page 1-33, leave the Ethernet test set hooked up to the Ethernet port in the source node.

b. If you are starting the current procedure without the Ethernet test set hooked up to the Ethernet port, use appropriate cabling to connect the Ethernet test set to the port you are testing.

Step 2 Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Use CTC to set up the hairpin circuit on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Hairpin1.

e. Choose the Size, such as STS-1.

f. Uncheck the **Bidirectional** check box. Leave the default values for State, SD Threshold, and SF Threshold.

g. Click **Next**.

h. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) where the test set is connected. Leave Use Secondary Source unchecked.

i. Click **Next**.

j. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box. Leave Use Secondary Destination unchecked.

k. Click **Next**.

l. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 3 Confirm that the newly created circuit appears on the Circuits tab and that the Dir column describes it as a one-way circuit.

Step 4 Complete the "Test and Delete the Ethernet Port Hairpin Circuit" procedure on page 1-37.

Test and Delete the Ethernet Port Hairpin Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the hairpin circuit. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Step 4 Complete the "Test the Standby Cross-Connect Card" procedure on page 1-38.

Test the Standby Cross-Connect Card

Note Two cross-connect cards (active and standby) must be in use on a node to use this procedure.

Step 1 Perform a reset on the Active cross-connect card to make the Standby card Active:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/SBY LED is amber and the active card ACT/SBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

d. Click **Yes** in the confirmation dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 3 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Step 4 To confirm a defective original cross-connect card, complete the "Retest the Original Cross-Connect Card" procedure on page 1-38.

Retest the Original Cross-Connect Card

Step 1 Initiate an external switching command (side switch) on the cross-connect cards:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/SBY LED is amber and the active card ACT/SBY LED is green.

b. In node view, select the **Maintenance > Cross-Connect > Cards** tabs.

c. From the Cross-Connect Cards menu, choose **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support at (1-800-553-2447) and proceed to Step 4. If the test does not indicate a faulty circuit, proceed to Step 5.

Step 4 Complete the "2.10.3 Physical Card Reseating and Replacement" procedure on page 2-163 for the defective card.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Step 6 Complete the "1.6.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-39.

1.6.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port

Performing the facility loopback test on an intermediate node OC-N port (which carries the Ethernet circuit) isolates whether this node is causing circuit failure. Complete the "Create a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-39.

Note The CE100T-8 Ethernet card only supports point-to-point configurations and is not directly implicated in the intermediate node testing.

Create a Facility Loopback on an Intermediate-Node OC-N Port

Step 1 Connect a test set to the OC-N port you are testing. If you are starting the current procedure without the test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the test set to the port you are testing. Both Tx and Rx connect to the same port.

Note For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

Step 2 Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Step 3 Use CTC to set up the facility loopback on the OC-N port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as C1CtoC1C3.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Step 5 Create the facility loopback on the destination port being tested:

a. Go to the node view of the intermediate node:

- Choose **View > Go To Other Node** from the menu bar.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the intermediate-node 15310-CL-CTX or CTX2500 card card where you will perform the loopback.

c. Click the **Maintenance > Optical > Loopback > Port** tabs.

d. Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

e. Select **Facility** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

Note It is normal for the "LPBKFACILITY (OCN)" condition on page 2-111. The condition clears when you remove the loopback.

Step 6 Complete the "Test and Clear the OC-N Facility Loopback Circuit" procedure on page 1-40.

Test and Clear the OC-N Facility Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback from the port:

a. Double-click the 15310-CL-CTX or CTX2500 card card and click the **Maintenance > Optical > Loopback > Port** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 4 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the OC-N (Controller) Card" procedure on page 1-41.

Test the OC-N (Controller) Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-163 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card installed.

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1-800-553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-163 for the faulty card.

Step 5 Clear the facility loopback from the port:

a. Double-click the card and click the **Maintenance > Optical > Loopback > Port** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.6.5 Perform a Terminal Loopback on Intermediate-Node OC-N Ports" procedure on page 1-42.

1.6.5 Perform a Terminal Loopback on Intermediate-Node OC-N Ports

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. To do this, you create a bidirectional circuit that originates on the source-node Ethernet port and loops back on the intermediate-node port. You then proceed with the terminal loopback test. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Caution Performing a loopback on an in-service circuit is service-affecting.

Note Terminal loopbacks require on-site personnel.

Complete the "Create a Terminal Loopback on Intermediate-Node OC-N Ports" procedure on page 1-42.

Create a Terminal Loopback on Intermediate-Node OC-N Ports

Step 1 Connect a test set to the 15310-CL-CTX or CTX2500 card port you are testing:

Note For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

a. If you just completed the "1.6.4 Perform a Facility Loopback on an Intermediate-Node OC-N Port" procedure on page 1-39 for the Ethernet circuit, leave the test set hooked up to the intermediate-node port.

b. If you are starting the current procedure without the test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the test set to the port you are testing. Both Tx and Rx connect to the same port.

Step 2 Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Step 3 Use CTC to set up the terminal loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as C1C1toC1C4.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list and that it is described in the Dir column as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (OCN)" condition on page 2-113 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal loopback on the destination port being tested:

a. Go to the node view of the intermediate node:

- Choose **View > Go To Other Node** from the menu bar.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the 15310-CL-CTX or CTX2500 card that requires the loopback.

c. Click the **Maintenance > Optical > Loopback > Port** tabs.

d. Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

e. Select **Terminal** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Test and Clear the OC-N Terminal Loopback Circuit" procedure on page 1-43.

Test and Clear the OC-N Terminal Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the terminal loopback from the port:

a. Double-click the intermediate-node 15310-CL-CTX or CTX2500 card with the terminal loopback to display the card view.

b. Click the **Maintenance > Optical > Loopback > Port** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the OC-N Card" procedure on page 1-44.

Test the OC-N Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-163 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card.

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1-800-553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-163 for the defective card.

Step 5 Clear the terminal loopback on the port:

a. Double-click the source-node 15310-CL-CTX or CTX2500 card with the terminal loopback.

b. Click the **Maintenance > Optical > Loopback > Port** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.6.6 Perform a Facility Loopback on a Destination-Node Ethernet Port" procedure on page 1-45.

1.6.6 Perform a Facility Loopback on a Destination-Node Ethernet Port

You perform a facility loopback test at the destination port to determine whether this local port is the source of circuit trouble.

Caution Performing a loopback on an in-service circuit is service-affecting.

Note Facility loopbacks require on-site personnel.

Complete the "Create the Facility Loopback on a Destination-Node Ethernet Port" procedure on page 1-45.

Create the Facility Loopback on a Destination-Node Ethernet Port

Step 1 Connect a test set to the CE100T-8 card that you are testing:

Note For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

a. If you just completed the "1.6.5 Perform a Terminal Loopback on Intermediate-Node OC-N Ports" section on page 1-42, leave the test set hooked up to the source-node port.

b. If you are starting the current procedure without the test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the test set to the port you are testing. Both Tx and Rx connect to the same port.

Step 2 Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Step 3 Use CTC to set up the hairpin circuit on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as C1C1toC1C5.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the 2.7.163 LPKTERMINAL (CE100T, CEMR) to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the facility loopback on the destination port being tested:

a. Go to the node view of the destination node:

- Choose **View > Go To Other Node** from the menu bar.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the CE100T-8 card that requires the loopback.

c. Click the **Maintenance > Loopback** tabs.

d. Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

e. Select **Facility** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Test and Clear the Ethernet Facility Loopback Circuit" procedure on page 1-46.

Test and Clear the Ethernet Facility Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback from the port:

a. Double-click the CE100T-8 card and click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 4 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-47.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-163 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card installed.

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1-800-553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-163 for the faulty card.

Step 5 Clear the facility loopback on the port:

a. Double-click the CE100T-8 card and click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.6.7 Perform a Terminal Loopback on a Destination-Node Ethernet Port" procedure on page 1-48.

1.6.7 Perform a Terminal Loopback on a Destination-Node Ethernet Port

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port.

Caution Performing a loopback on an in-service circuit is service-affecting.

Note Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal Loopback on a Destination-Node Ethernet Port" procedure on page 1-48.

Create the Terminal Loopback on a Destination-Node Ethernet Port

Step 1 Connect a test set to the CE100T-8 port that you are testing:

Note For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

a. If you just completed the "1.6.6 Perform a Facility Loopback on a Destination-Node Ethernet Port" procedure on page 1-45, leave the test set hooked up to the source port.

b. If you are starting the current procedure without the test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the test set to the port you are testing. Both Tx and Rx connect to the same port.

Step 2 Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Step 3 Use CTC to set up the terminal loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as C1C1toC1C6.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPKTERMINAL (CE100T, CEMR)" condition on page 2-111 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal loopback on the destination port being tested:

a. Go to the node view of the destination node:
   - Choose **View > Go To Other Node** from the menu bar.
   - Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the CE100T-8 card that requires the loopback.

c. Click the **Maintenance > Loopback** tabs.

d. Select **OOS,MT** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

e. Select **Terminal** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Test and Clear the Ethernet Terminal Loopback Circuit" procedure on page 1-49.

Test and Clear the Ethernet Terminal Loopback Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Clear the terminal loopback from the port:

a. Double-click the intermediate-node CE100T-8 card with the terminal loopback.

b. Click the **Maintenance > Loopback** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

The entire circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the Ethernet Card" procedure on page 1-50.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Card" procedure on page 2-163 for the suspected bad card and replace it with a known-good card.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 Resend test traffic on the loopback circuit with a known-good card.

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1-800-553-2447).

Step 4 Complete the "Physically Replace a Card" procedure on page 2-163 for the defective card.

Step 5 Clear the terminal loopback on the port:

a. Double-click the source-node CE100T-8 card with the terminal loopback.

b. Click the **Maintenance > Loopback** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

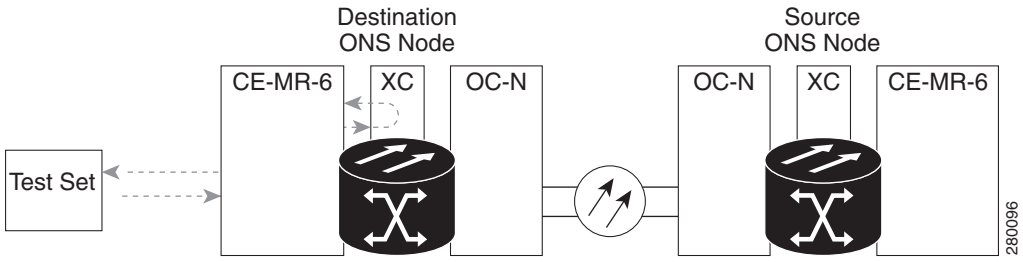
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

The entire circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

1.6.8 Perform a Hairpin Test on a Destination-Node Ethernet Port

The hairpin test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port as source as well as destination. Completing a successful hairpin through the card isolates the possibility that the cross-connect card is the cause of the faulty circuit. Figure 1-7 shows an example of a hairpin loopback on a destination-node port.

Figure 1-7 Hairpin on a Destination-Node Ethernet Port



Note The ONS 15310-MA does not support simplex operation on the cross-connect card. Two cross-connect cards of the same type must be installed for each node.

Note Hairpin loopbacks require on-site personnel.

Complete the "Create the Hairpin Circuit on the Destination-Node Port" procedure on page 1-51.

Create the Hairpin Circuit on the Destination-Node Port

Step 1 Connect an Ethernet test set to the port you are testing:

a. If you just completed the "1.6.7 Perform a Terminal Loopback on a Destination-Node Ethernet Port" procedure on page 1-48, leave the Ethernet test set hooked up to the Ethernet port in the destination node.

b. If you are starting the current procedure without the Ethernet test set hooked up to the Ethernet port, use appropriate cabling to connect the Ethernet test set to the port you are testing.

Step 2 Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Step 3 Use CTC to set up the hairpin circuit on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Hairpin1.

e. Choose the Size, such as STS-1.

f. Uncheck the **Bidirectional** check box. Leave the default values for State, SD Threshold, and SF Threshold.

g. Click **Next**.

h. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) where the test set is connected. Leave **Use Secondary Source** unchecked.

i. Click **Next**.

j. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box. Leave **Use Secondary Destination** unchecked.

k. Click **Next**.

l. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab and that the Dir column describes it as a one-way circuit.

Step 5 Complete the "Test and Delete the Ethernet Hairpin Circuit" procedure on page 1-52.

Test and Delete the Ethernet Hairpin Circuit

Step 1 If the test set is not already sending traffic, send test traffic on the loopback circuit.

Step 2 Examine the test traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

Step 3 If the test set indicates a good circuit, no further testing is necessary with the hairpin circuit. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Step 4 Complete the "Test the Standby Cross-Connect Card" procedure on page 1-52.

Test the Standby Cross-Connect Card

Note Two cross-connect cards (active and standby) must be in use on a node to use this procedure.

Step 1 Perform a reset on the Active cross-connect card to make the Standby card Active:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/SBY LED is amber and the active card ACT/SBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

d. Click **Yes** in the confirmation dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 3 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

Step 4 To confirm a defective original cross-connect card, complete the "Retest the Original Cross-Connect Card" procedure on page 1-53.

Retest the Original Cross-Connect Card

Step 1 Initiate an external switching command (side switch) on the cross-connect cards:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/SBY LED is amber and the active card ACT/SBY LED is green.

b. In node view, select the **Maintenance > Cross-Connect > Cards** tabs.

c. From the Cross-Connect Cards menu, choose **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/SBY LED turns green. The former active card becomes standby and its ACT/SBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the return materials authorization (RMA) process. Contact Cisco Technical Support at (1-800-553-2447) and proceed to Step 4. If the test does not indicate a faulty circuit, proceed to Step 5.

Step 4 Complete the "2.10.3 Physical Card Reseating and Replacement" procedure on page 2-163 for the defective cross-connect card.

Step 5 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted from the Circuits tab list.

The entire circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

1.7 Verify Wiring from the ONS 15310-MA Shelf and DSX Wiring Panel

This procedure verifies the DS-1 and DS-3 wiring between the backplane of an ONS 15310-MA shelf and the digital signal cross-connect (DSX) wiring panel. The procedure is normally used in new installations before the cards have been installed and while the shelf is still powered down.

Note Before performing this procedure, the TST-DSX card must be installed in the Cisco ONS 15310-MA shelf. Refer to the "Install the Cisco ONS 15310-MA" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for instructions.

Caution There must be no DS-1 or DS-3 traffic in the side of the shelf being tested. The TST-DSX card disrupts service if it is plugged into the companion slot of a shelf side where a DS-1 or DS-3 port is already carrying traffic on that same side.

1.7.1 Set Up the Equipment for Testing

Step 1 Install the TST-DSX card in the ONS 15310-MA shelf and prepare the handheld receiver as described in the "Install the Cisco ONS 15310-MA" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide.*

Note The TST-DSX card may be installed only in Slots 1 or 2 of the "A" side of the shelf or Slots 5 or 6 of the "B" side.

Note The TST-DSX card receives power either from the shelf or from the supplied AC-to-DC converter.

Note The TST-DSX card sends signals to the handheld receiver over the DS-1 and DS-3 cable bundles on both the IN and OUT ports as labeled on the DSX wiring panel. The handheld receiver is designed to function as a single-location testing device at the DSX panel for all IN and OUT DS-1 and DS-3 ports.

Figure 1-8 shows the test setup.

Figure 1-8 TST-DSX and Remote Receiver Faceplates

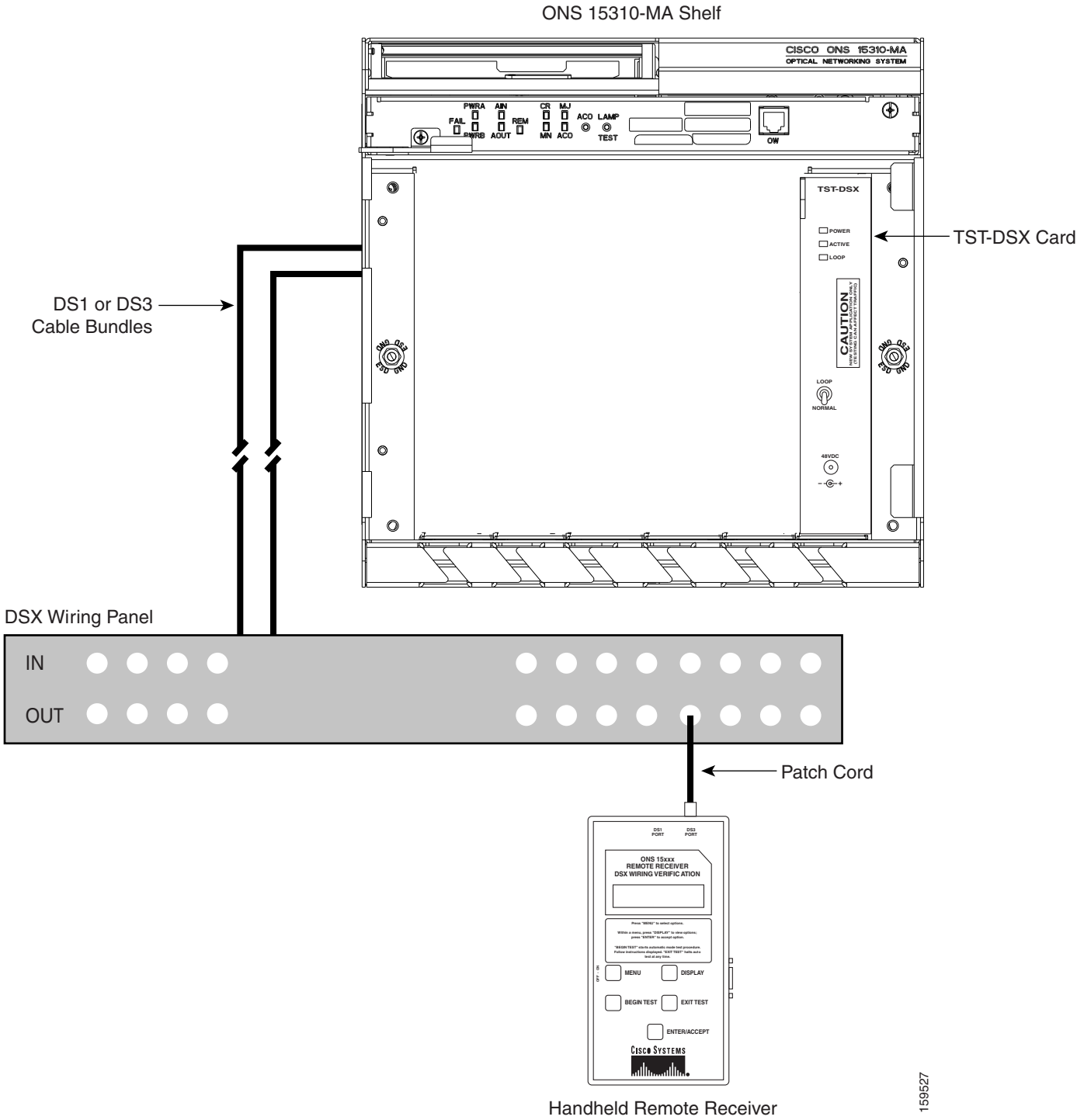
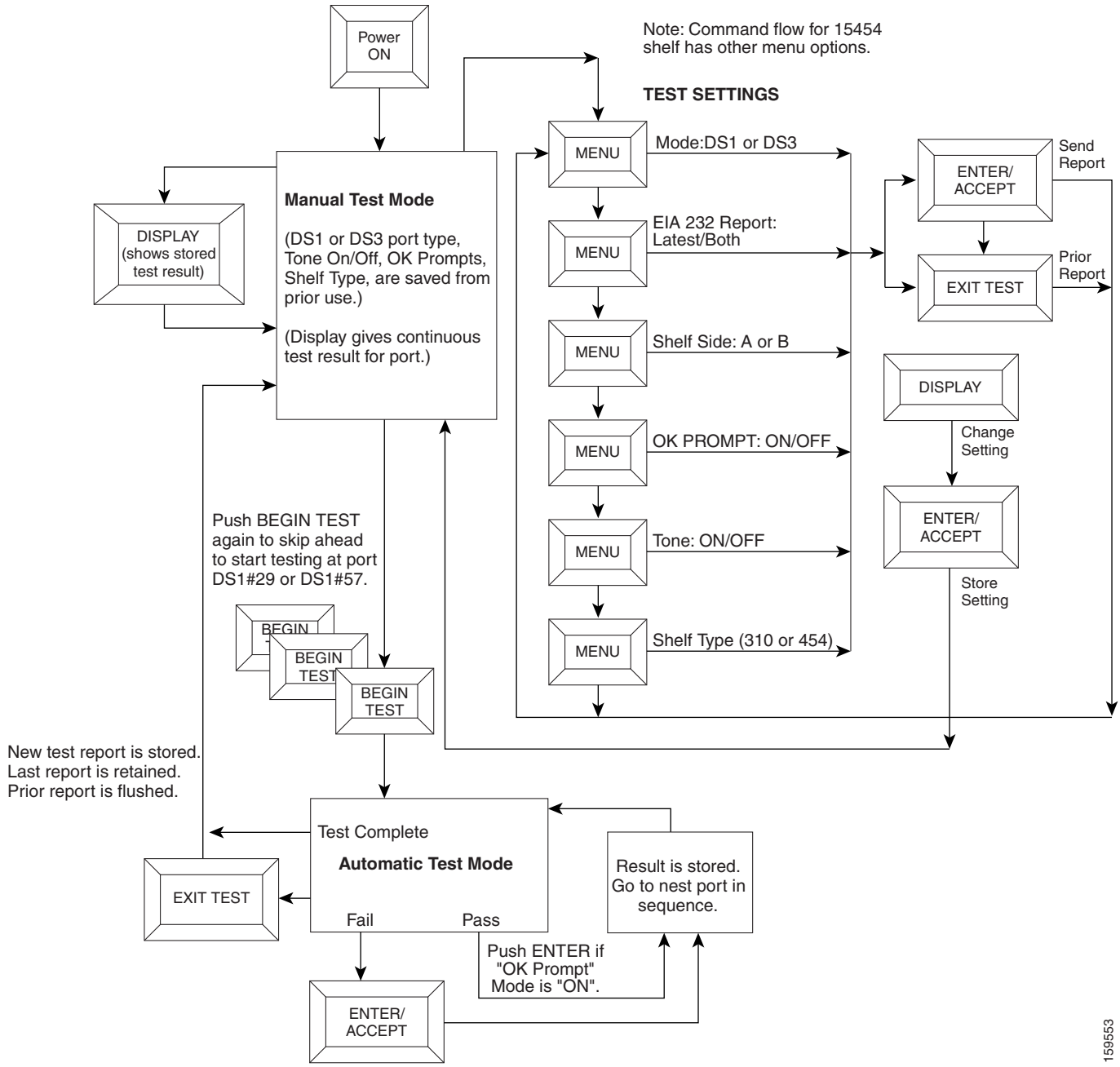


Figure 1-9 shows how to use the handheld receiver to perform various tests.

Figure 1-9 Handheld Receiver Usage Flowchart



Step 2 Connect a patch cord between the DS1 Port or DS3 Port connector on the handheld receiver and the desired port of the DSX panel.

The following patch cords are available

- DS-3 patch cords
  - 75-ohm male BNC connector to male WECo 440A male connector
  - 75-ohm male BNC connector to WECo 358 male connector
  - 75-ohm male BNC connector to 75-ohm male BNC connector

  - 75-ohm male BNC connector to LCP connector
- DS1 patch cords
  - 100-ohm male Bantam connector to 100-ohm male Bantam connector
  - 100-ohm male Bantam connector to 100-ohm 310 connector

Step 3 Complete the "1.7.2 Perform Manual Mode Tests" procedure on page 1-57 or the "1.7.3 Perform Automatic Mode Tests" procedure on page 1-59, as needed.

1.7.2 Perform Manual Mode Tests

The manual mode test allows you to plug the patch cord from the appropriate connector on the handheld receiver (DS1 Port or DS3 Port) into a connector on the DSX panel. The handheld receiver then displays the result of the test. The manual mode is useful for debugging a small number of wiring connections.

1.7.2.1 Set Up the Handheld Receiver for Manual Mode Testing

This section describes how to set up the 15xxx RR handheld receiver to test individual wire connections. Figure 1-9 shows how to move from one option setting to another with the handheld receiver.

Step 1 Turn the handheld receiver unit on using the OFF- ON switch on the left side of the unit and observe the display.

Step 2 After the display has stopped changing, you will see that it is in manual mode with the settings last used, either DS-1 or DS-3.

Step 3 To change to a different cable type (DS-1 or DS-3), press the **MENU** key once.

Step 4 While the MENU screen is being displayed, press the **DISPLAY** key to change the setting and the **ENTER** key to store the setting.

Step 5 Complete the "1.7.2.2 Perform Manual Tests" procedure on page 1-57, as needed.

1.7.2.2 Perform Manual Tests

Step 1 At the DSX wiring panel, insert a appropriate patch cord into the handheld receiver.

Step 2 Insert the other end of the patch cord into a port on the DSX panel. The handheld receiver's screen continuously shows the test result of any detected signal.

Step 3 Review the "1.7.2.3 View and Troubleshoot Manual Test Results" section on page 1-58.

1.7.2.3 View and Troubleshoot Manual Test Results

The handheld receiver screen displays the test result for one DSX port and its DSX wiring, as shown in Table 1-1. Each port is uniquely identified and reported. If a test signal generated from the TST-DSX card is properly detected, the handheld receiver decodes the signal and the screen displays the port type and number and gives an OK indication. Detected errors also appear on the handheld receiver screen. Test results are not stored in the handheld receiver memory during Manual mode.

Much like a voltmeter, the handheld receiver displays what it sees. The handheld receiver reports a "good" port signal whenever it detects a properly encoded signal at its input; it has no knowledge of any labels at the DSX panel. For example, if the wires of a good signal for port A:12 are wrongly cross-wired to the DSX port labeled B:84, the handheld receiver only reports what it sees: port A:12 is "good."

While the handheld receiver is in the manual mode, the **EXIT TEST** or **ENTER/ACCEPT** keys have no effect.

Table 1-1 Messages and Probable Indications

General Indication	Definition and Probable Cause	Specific Sample Message	Definition and Probable Cause
OK	The handheld receiver detects a valid signal from the TST-DSX card, indicating the wiring is correct.	INP DS1 B:42 OK	Input B side, port 42 for DS-1 is detected and tests good.
OPEN/NC	There is no signal at the input to the handheld receiver. When the handheld receiver is first powered up and before any patch cord is inserted into the unit, the Open/NC message is given. This message also appears if a wire is broken from the shelf to the DSX or if a "split pair" error is made where, for example, a "TIP" of one port and a "RING" of another port are both wired to the same DSX port appearance. Also, if the TST- DSX is not powered or not inserted into the shelf, no signals are generated.	DS1 OPEN/NC	There is no signal at the input to the handheld receiver.
I, IN or INP	An input port. A DS I or DS-3 service signal, if present, would flow from the DSX to the shelf.	INP DS1 B:42 OK	Input B side, port 42 for DS-1 is detected and tests good.
O or OUT	An output port. A DS-1 or DS-3 service signal, if present, would flow from the shelf to the DSX.	OUT DS1 A: 5 OK	Output A side, port 5 for DS I is detected and tests good.
SHORT	The handheld receiver detects that the TIP and RING of a DS-1 are shorted together, or the DS-3 center conductor is shorted to its shield or frame ground.	DS1 SHORT	The Tip and Ring of a DS-1 port are shorted together.
UNIDENT	An unidentified signal is detected.	DS1 UNIDENTIFIED	The signal is not valid for the 15310-MA shelf.
INR or REV	For DS-1 input wires: Tip and Ring reversal.	DS1 => INP A:11 REV	DS-1 input A side, port 11 is detected, but the tip and ring are reversed.

Table 1-1 Messages and Probable Indications (continued)

General Indication	Definition and Probable Cause	Specific Sample Message	Definition and Probable Cause
OUTR or REV	For DS-1 output wires: Tip and Ring reversal.	DS1 => OUT A:10 REV	DS 1 output A side, port 10 is detected, but the tip and ring are reversed.
WE or WIRE ERR	A wiring error is detected. WIRE ERR appears on the handheld receiver if the detected signal cannot be diagnosed. There are cases, such as when two or more wires shorted together, where WIRE ERROR is the only indication the handheld receiver can display.	—	—

1.7.3 Perform Automatic Mode Tests

This section describes how to use the 15xxx RR handheld receiver to perform a series of tests that span one or more groups of shelf wiring. With the handheld receiver you can also view and record test results. The handheld receiver guides you through the port numbers.

There are two types of automatic mode tests:

- True automatic mode
- Manual prompt mode

The handheld receiver ships with the true automatic mode as the default selection.

1.7.3.1 True Automatic Mode

In the true automatic mode, you are directed to go to the first port in the testing sequence. As soon as the handheld receiver detects the expected signal, the measurement is recorded in memory, the handheld receiver emits a beep, and you are directed to the next port. Testing can be done without looking at the handheld receiver display for the entire DSX panel; you simply listen for the sound of the successful beep and then plug the patch cord into each successive port. If any port fails during the test, the handheld receiver displays the error and waits for you to press the **ENTER/ACCEPT** key to save the result. When the error is recorded, the handheld receiver beeps and the next test port is displayed.

1.7.3.2 Manual Prompt Mode

The manual prompt mode is activated by pressing the **MENU** key four times and using the **DISPLAY** key to switch to the manual **OK PROMPT** mode. You are directed to go to the first port in the testing sequence. The handheld receiver displays the expected input port and the detected signal, either OK or faulty, but then waits for you to press the **ENTER/ACCEPT** key. After you press the key, the handheld receiver records the measurement, beeps, and then prompts for the next port to measure. You must press the **ENTER /ACCEPT** key for every measurement made, both for OK and for errors, up to 84 times for a full shelf side of DSl signals.

1.7.3.3 Provision the Handheld Receiver and Perform Automatic Mode Testing

Step 1 Turn on the handheld receiver and observe the display. Adjust the settings (DS l/DS3 or OK PROMPT) as needed:

a. To change from DS-1 to DS-3 or from DS-3 to DS-1, press the **MENU** key once, use the **DISPLAY** key to change the selection, and the **ENTER/ACCEPT** key to save the selection.

b. To change the OK PROMPT setting, press the MENU key four times, use the **DISPLAY** key to change the selection, and the **ENTER/ACCEPT** key to save the selection

Step 2 To set the audible tone ON, press the **MENU** key five times, use the **DISPLAY** key to change the selection, and the **ENTER/ACCEPT** key to save the selection

Step 3 Insert an appropriate patch cord into the handheld receiver.

Step 4 At this point, the handheld receiver is still in the manual mode. Press the **BEGIN TEST** key to enter the automatic mode.

Note Pushing the **BEGIN TEST** key when testing DS-1 wiring starts the automatic test mode at DS-1 port 1 and continues for all 84 ports. To start testing at the DS-1 ports of the second connector pair, ports 29 to 56, push the **BEGIN TEST** key a second time, and the handheld receiver skips ahead to prompt for the DS I port 29. Pushing **BEGIN TEST** a third time advances the handheld receiver to start testing at the last DS-1 group, DS 1 port 57.

At any time, you may press EXIT TEST, which terminates the automatic test mode, stores the results thus far, and returns the handheld receiver to the manual mode. This is a convenient feature that, along with the skip ahead feature, allows automatic testing and result storage for a portion of the shelf's connector wiring.

Step 5 Insert the other end of the patch cord into the requested port shown on the display screen.

Step 6 Wait a few seconds for the handheld receiver to detect the signal. For a good measurement in full automatic mode, the handheld receiver displays OK, beeps, and then shows the next port to test.

Step 7 If there is an error, or if the OK PROMPT mode is active, press the **ENTER/ACCEPT** key to store the result.

Step 8 Move the patch cord to the next port to be tested, as shown in the GOTO message on the display.

Step 9 Repeat Step 5 through Step 8 until all ports are tested.

Note Press the **EXIT TEST** key to abort the testing at any time. The results to that point are stored in memory, and the handheld receiver reverts to manual mode.

1.7.3.4 View Automatic Mode Test Results During the Test

During the automatic test, there are many test conditions and messages that can appear. A few examples are given in Table 1-2 for DS-1 signal ports. Similar messages appear for the DS-3 ports.

Table 1-2 Automatic Test Mode Results

Result	Meaning
GOTO A:15 OUT	The next port to be tested is side A, port 15 OUT direction. This prompt is displayed in the upper half of the screen.
DS1 OPEN OR NC	The handheld receiver does not detect any signal. This message is displayed and alternates on the bottom half of the screen.
ENTER TO ACCEPT	The user is asked to press the **ENTER/ACCEPT** key to record the present test result. This message appears at the bottom half of the screen and alternates with a test result.
OUT DS I A:15 OK	Output cable side A, port 15 for DS-1 is detected correctly. This message alternates on the lower half of the display screen. In true automatic mode, this test result flashes only until the handheld receiver stores the result in memory and then the handheld receiver beeps success and shows the next port in the GOTO message at the top half of the display. In the manual prompt mode, the handheld receiver alternates this message with the **ENTER/ACCEPT** message until the user pushes the **ENTER** key.
I A: I 5=>O A: 15	Output port A:15 is detected instead of the expected input port A:15. This test result message alternates on the lower half of the screen. This “error” could occur if the user has not yet moved the test cord from the output port just tested to the next port in sequence, the input port. The printed report for this error would appear as A: 15 WE=>OUT A: 15.
1 B: 17=>O B: 8	DS-1 output side B8 is detected, but the handheld receiver was expecting input group B port 17. This test result message alternates on the lower half of the display. The printed report would record this as B: 17 WE=>OUT B: 8.
O A:18=>OR A:12	DS-1 output A port 12 is detected, but the tip and ring are reversed, and the handheld receiver was expecting output A port 18. This test result message alternates on the lower half of the display. The printed report would record this as A: 18 WE=>OUTR A: 12.
DS 1 SHORT	The message flashes on the lower half of the display to indicate that the Tip and Ring of a DS-1 port are shorted together.
DS I WIRE ERROR	This message flashes on the lower half of the display to indicate the detected signal cannot be diagnosed. There are cases, such as when two or more wires shorted together, where WIRE ERROR is the only indication the handheld receiver can display.
TEST COMPLETE	The automatic mode has finished testing all the ports in the sequence, or the user has halted the testing by pushing the **EXIT TEST** key.
DISPLAY TO VIEW	When the test has stopped, the user can review the results on the screen by pressing the **DISPLAY** key.

1.7.4 Retrieving Test Results from Automatic Tests

The results of the last two automated tests can be viewed on the handheld receiver display screen or a computer connected via the handheld receiver’s EIA-232 port. Two test reports are stored in the handheld receiver's memory. When a third automatic test is started, the older of the two stored tests is erased. Only the two most recent tests are stored at any time. You may clear memory by pushing BEGIN TEST and then END TEST.

1.7.4.1 Reviewing the Results on the Handheld Receiver Screen

At the conclusion of the automatic test or if you press the EXIT TEST key, the handheld receiver enters the manual mode. Press DISPLAY to recall on the screen the last automated test results. Only "failed" ports are shown. Ports that either pass or are untested do not appear on the screen. Each time the DISPLAY key is pressed, the next test result appears.

1.7.4.2 Sending the Results to a Computer

After the automatic test is complete and the handheld receiver is again in manual mode, the handheld receiver can send the stored results to a computer. The report is in the form of a standard text file.

Step 1 Using the supplied cable with DB9 female connectors at each end, connect the handheld receiver's EIA 232 port to a computer.

Note The handheld receiver operates as a data communications equipment (DCE) device. A straight through DB9 cable is used (pin 2 to pin 2, pin 3 to pin 3, pin 5 to pin 5).

Step 2 Set up the computer's serial port for 9600 baud, 8 data bits, no parity, and one stop bit.

Note See the instructions for your computer for the appropriate software and terminal mode set up.

Step 3 Press the **MENU** key once. The DSX wiring selection menu appears.

Step 4 Press **MENU** a second time. The test report menu appears.

Step 5 Press **ENTER/ACCEPT** to send the test result out the EIA 232 port.

Step 6 Wait for completion, or press **EXIT TEST** to abort the report. At 9600 baud the report takes only a few seconds to transmit. Either the most recent or both stored reports can be sent.

The handheld receiver returns to manual mode. Each port will have a result, either "OK," an error result, or "UNTESTED." The test reports are stored in non-volatile memory and saved until overwritten by the next test activity; this allows you to power down the handheld receiver while retaining the reports for later transmission to a computer.

There are blank lines in the test report format that you can edit to enter name, time, date, shelf locations, and so on. The test report text file may be edited with any convenient software program after being sent to a computer.

1.7.5 Perform Loop Tests

The TST-DSX card has limited capability for loopback testing with a commercial DS-1 or DS-3 test set. The handheld receiver is not used in the LOOP testing mode.

The TST DSX has passive loop circuitry with no recovery and regeneration of signals. The loop path through the ONS 15310-MA shelf and the TST-DSX card has insertion loss, which reduces the voltage amplitude of a looped signal. The cable length between the DSX wiring panel and the shelf also

introduces insertion loss. Depending on the total insertion loss and the receive sensitivity threshold of the test set, it may not always be possible for a given test set to recover the weakened signal at maximum cable lengths.

Step 1 At the ONS 15310-MA shelf, set the TST-DSX card front panel switch to the **LOOP** position. The LOOP LED turns steady on and the ACTIVE LED blinks.

Step 2 Connect the DS-1 or DS-3 TX/OUT signal of a commercial test set to the desired input jack at the DSX panel and connect the DSX OUT jack to the commercial test set RCV/IN port.

Note For each signal port, the TST-DSX card loops the IN port to the OUT port. That is, IN port 1 is looped to OUT port 1, port 2 to port 2, and so on. Because of the insertion loss in each looped port, daisy chaining of signals is not supported.

Note The commercial test set should show error free transmission. However, the return signal level is at a reduced level.

1.8 Restore the Database and Default Settings

This section contains troubleshooting procedures for errors that require restoration of software data or the default node setup.

1.8.1 Restore the Node Database

Symptom One or more nodes are not functioning properly or have incorrect data.

Table 1-3 describes the potential cause of the symptom and the solution.

Table 1-3 Restore the Node Database

Possible Problem	Solution
Incorrect or corrupted node database.	Complete the applicable procedures in the “Maintain the Node” chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

1.9 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and Java Runtime environments (JREs) for Software Release 9.0, and troubleshooting procedures for Microsoft Windows PC and network connectivity to the ONS 15310-CL or ONS 15310-MA.

1.9.1 Microsoft Windows PC System Minimum Requirements

Workstations running CTC Software R9.0 for the ONS products on Microsoft Windows platforms need to have the following minimum requirements:

- Pentium III or higher processor
- Processor speed of at least 700 MHz
- 256 MB or more of RAM
- 50 MB or more of available hard disk space
- 20 GB or larger hard drive

1.9.2 Sun, Solaris, or UNIX System Minimum Requirements

Workstations running CTC Software R9.0 for the ONS products on Sun, Solaris, or UNIX workstations need to have the following minimum requirements:

- UltraSPARC or faster processor
- 256 MB or more of RAM
- 50 MB or more of available hard disk space

1.9.3 Supported Platforms, Browsers, and JREs

CTC Software R9.0 supports the following platforms:

- Microsoft Windows NT
- Microsoft Windows 98
- Microsoft Windows XP
- Microsoft Windows 2000
- Sun, Solaris, or UNIX 8
- Sun, Solaris, or UNIX 9
- Sun, Solaris, or UNIX 10
- Microsoft Windows Vista

CTC Software R9.0 supports the following browsers and JREs:

- Netscape 7 browser (on Sun, Solaris, or UNIX 8 or 9 with Java plug-in 1.4.2 or 5.0)
- Microsoft Windows PC platforms with Java plug-in 1.4.2 or 5.0
- Internet Explorer 6.0 browser (on Microsoft Windows PC platforms with Java plug-in 5.0)
- Mozilla application suite for browsers

Note The supported browser can be downloaded from the Web.

Note The required JRE version for Software R9.0 is JRE 5.0.

Note JRE 5.0 for Microsoft Windows and Sun (Solaris, UNIX) is available on Software R9.0 product CDs.

1.9.4 Unsupported Platforms and Browsers

Software R9.0 does not support the following platforms:

- Microsoft Windows 95
- Sun, Solaris, or UNIX 2.5
- Sun, Solaris, or UNIX 2.6

Software R9.0 does not support the following browsers and JREs:

- Netscape 4.73 for Microsoft Windows.
- Netscape 4.76 on Sun, Solaris, or UNIX is not supported.

1.9.5 Unable to Verify the IP Configuration of Your Microsoft Windows PC

Symptom When connecting your Microsoft Windows PC to the ONS 15310-CL or ONS 15310-MA, you are unable to successfully ping the IP address of your Microsoft Windows PC to verify the IP configuration.

Table 1-4 describes the potential causes of the symptom and the solutions.

Table 1-4 Unable to Verify the IP Configuration of Your Microsoft Windows PC

Possible Problem	Solution
The IP address is typed incorrectly.	Verify that the IP address used to ping the Microsoft Windows PC matches the IP address displayed when the Microsoft Windows IP Configuration information is retrieved from the system.
The IP configuration of your Microsoft Windows PC is not properly set.	Verify the IP configuration of your Microsoft Windows PC, see the "Verify the IP Configuration of Your Microsoft Windows PC" procedure on page 1-65. If this procedure is unsuccessful, contact your network administrator for instructions to correct the IP configuration of your Microsoft Windows PC.

Verify the IP Configuration of Your Microsoft Windows PC

Step 1 Open a DOS command window by selecting **Start > Run** from the Start menu.

Step 2 In the Open field, type **command** and then click **OK**. The DOS command window appears.

Step 3 At the prompt in the DOS window (or Microsoft Windows 98, NT, 2000, and XP), type **ipconfig** and press the **Enter** key.

The Microsoft Windows IP configuration information appears, including the IP address, subnet mask, and the default gateway.

Step 4 At the prompt in the DOS window, type **ping** followed by the IP address shown in the Microsoft Windows IP configuration information.

Step 5 Press the **Enter** key to execute the command.

If the DOS window displays multiple (usually four) replies, the IP configuration is working properly.

If you do not receive a reply, your IP configuration might not be properly set. Contact your network administrator for instructions to correct the IP configuration of your Microsoft Windows PC.

1.9.6 Browser Login Does Not Launch Java

Symptom The message "Loading Java Applet" does not appear and the JRE does not launch during the initial login.

Table 1-5 describes the potential causes of the symptom and the solutions.

Table 1-5 Browser Login Does Not Launch Java

Possible Problem	Solution
The Microsoft Windows PC operating system and browser are not properly configured.	Reconfigure the Microsoft Windows PC operating system java plug-in control panel and the browser settings. See the "Reconfigure the Microsoft Windows PC Operating System Java Plug-in Control Panel" procedure on page 1-66 and the "Reconfigure the Browser" procedure on page 1-67.

Reconfigure the Microsoft Windows PC Operating System Java Plug-in Control Panel

Step 1 From the Microsoft Windows start menu, click **Settings > Control Panel**.

Step 2 If **Java Plug-in Control Panel** does not appear, the JRE might not be installed on your Microsoft Windows PC.

- **a.** Run the Cisco ONS 15310-CL or ONS 15310-MA software CD.
- **b.** Open the *CD-drive*:\Windows\JRE folder.
- **c.** Double-click the **j2re-5_0-win** icon to run the JRE installation wizard.
- **d.** Follow the JRE installation wizard steps.

Step 3 From the Microsoft Windows start menu, click **Settings > Control Panel**.

Step 4 In the Java Plug-in Control Panel window, double-click the **Java Plug-in 5.0**) icon.

Step 5 Click the **Advanced** tab on the Java Plug-in Control Panel.

Step 6 From the Java Run Time Environment menu, select **JRE 5.0 in C:\ProgramFiles\JavaSoft\JRE\5.0**.

Step 7 Click **Apply**.

Step 8 Close the Java Plug-in Control Panel window.

Reconfigure the Browser

Step 1 From the Microsoft Windows Start menu, launch your browser application.

Step 2 If you are using Netscape Navigator:

a. From the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

b. In the Preferences window, click the **Advanced > Proxies** categories.

c. In the Proxies window, click the **Direct connection to the Internet** check box and click **OK**.

d. From the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

e. In the Preferences window, click the **Advanced > Cache** categories.

f. Confirm that the Disk Cache Folder field shows one of the following paths:

- For Microsoft Windows 98/ME, C:\ProgramFiles\Netscape\Communicator\cache
- For Microsoft Windows NT/2000/XP, C:\ProgramFiles\Netscape*username*\Communicator\cache

g. If the Disk Cache Folder field is not correct, click the **Choose Folder** button.

h. Navigate to the file listed in Step f and click **OK**.

i. Click **OK** in the Preferences window and exit the browser.

Step 3 If you are using Internet Explorer:

a. On the Internet Explorer menu bar, click the **Tools > Internet Options** menus.

b. In the Internet Options window, click the **Advanced** tab.

c. In the Settings menu, scroll down to Java (Sun, Solaris, or UNIX) and click the **Use Java 2 v1.4.2 for** *applet* **(requires restart)** check box (or the **Use Java 2 v5.0 for** *applet* **(requires restart)** check box).

d. Click **OK** in the Internet Options window and exit the browser.

Step 4 Temporarily disable any virus-scanning software on the computer. See the "1.10.3 Browser Stalls When Downloading CTC JAR Files from port" section on page 1-71.

Step 5 Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.

Step 6 Restart the browser and log into the ONS 15310-CL or ONS 15310-MA.

Step 7 After completing browser configuration, enable the virus-scanning software on the computer.

1.9.7 Unable to Verify the NIC Connection on Your Microsoft Windows PC

Symptom When connecting your Microsoft Windows PC to the ONS 15310-CL or ONS 15310-MA, you are unable to verify that the NIC connection is working properly because the link LED is not on or flashing.

Table 1-6 describes the potential causes of the symptom and the solutions.

Table 1-6 Unable to Verify the NIC Connection on Your Microsoft Windows PC

Possible Problem	Solution
The CAT-5 cable is not plugged in properly.	Confirm that both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced.
The CAT-5 cable is damaged.	Ensure that the cable is in good condition. If in doubt, use a cable known to be good. Often, cabling is damaged due to pulling or bending.
Incorrect type of CAT-5 cable is being used.	If you are connecting an ONS 15310-CL or ONS 15310-MA directly to your Microsoft Windows laptop/PC or a router, use a straight-through CAT-5 cable. When connecting the node to a hub or a LAN switch, use a crossover CAT-5 cable. For details on the types of CAT-5 cables, see the "1.12.2.1 Crimp Replacement LAN Cables" procedure on page 1-88.
The NIC is improperly inserted or installed.	If you are using a Personal Computer Memory Card International Association (PCMCIA)-based NIC, remove and reinsert the NIC to make sure the NIC is fully inserted. If the NIC is built into the Microsoft Windows laptop/PC, verify that the NIC is not faulty.
The NIC is faulty.	Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), then the NIC should be working correctly. If you have difficulty connecting to the network (or any other node), then the NIC might be faulty and needs to be replaced.

1.9.8 Verify Microsoft Windows PC Connection to the Node (Ping)

Symptom The TCP/IP connection is established and then lost, and a DISCONNECTED alarm appears in CTC.

Table 1-7 describes the potential cause of the symptom and the solution.

Table 1-7 Verify Microsoft Windows PC Connection to ONS 15310-CL or ONS 15310-MA (Ping)

Possible Problem	Solution
A lost connection between the Microsoft Windows PC and the ONS 15310-CL or ONS 15310-MA.	Use a standard ping command to verify the TCP/IP connection between the Microsoft Windows PC and the ONS 15310-CL or ONS 15310-MA port. A ping command works if the Microsoft Windows PC connects directly to the port or uses a LAN to access the port. See the "Ping the ONS 15310-CL or ONS 15310-MA" procedure on page 1-69.

Ping the ONS 15310-CL or ONS 15310-MA

Step 1 Open the command prompt:

a. If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, type **command prompt** in the Open field of the Run dialog box, and click **OK**.

b. If you are using a Sun, Solaris, or UNIX operating system, from the Common Desktop Environment (CDE) click the **Personal Application tab** and click **Terminal**.

Step 2 For both the Sun (Solaris, UNIX) and Microsoft operating systems, at the prompt type:

```
ping ONS-15310-IP-address
```

For example:

```
ping 192.1.0.2
```

Step 3 If the workstation has connectivity to the node, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message appears.

Step 4 If the ping is successful, an active TCP/IP connection exists. Restart CTC.

Step 5 If the ping is not successful and the workstation connects to the node through a LAN, check that the workstation's IP address is on the same subnet as the ONS 15310-CL or ONS 15310-MA.

Step 6 If the ping is not successful and the workstation connects directly to the node, check that the link light on the workstation's NIC is illuminated.

1.10 CTC Operation Troubleshooting

This section contains troubleshooting procedures for CTC login or operation problems.

1.10.1 Unable to Launch CTC Help After Removing Netscape

Symptom After removing Netscape and running CTC using Internet Explorer, the user is unable to launch the CTC Help and receives an "MSIE is not the default browser" error message.

Table 1-8 describes the potential cause of the symptom and the solution.

Table 1-8 Unable to Launch CTC Help After Removing Netscape

Possible Problem	Solution
Loss of association between browser and Help files.	When the CTC software and Netscape are installed, the Help files are associated with Netscape by default. When you remove Netscape, the Help files are not automatically associated with Internet Explorer as the default browser. Set Internet Explorer as the default browser so that CTC will associate the Help files to the correct browser. See the "Set Internet Explorer as the Default Browser for CTC" procedure on page 1-70 to associate the CTC Help files to the correct browser.

Set Internet Explorer as the Default Browser for CTC

Step 1 Open the Internet Explorer browser.

Step 2 From the menu bar, click **Tools > Internet Options**. The Internet Options window appears.

Step 3 In the Internet Options window, click the **Programs** tab.

Step 4 Click the **Internet Explorer should check to see whether it is the default browser** check box.

Step 5 Click **OK**.

Step 6 Exit any and all open and running CTC and Internet Explorer applications.

Step 7 Launch Internet Explorer and open another CTC session. You should now be able to access the CTC Help.

1.10.2 Unable to Change Node View to Network View

Symptom Logging into CTC session, the user is unable to change node view to network view on any and all nodes, from any workstation. This is accompanied by an "Exception occurred during event dispatching: java.lang.OutOfMemoryError" in the java window.

Table 1-9 describes the potential cause of the symptom and the solution.

Table 1-9 Unable to Change Node View to Network View

Possible Problem	Solution
The browser stalls when downloading files from a port because the display requires more memory for the graphical user interface (GUI) environment variables.	Reset the system or user CTC_HEAP environment variable to increase the memory limits. See the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Microsoft Windows" procedure on page 1-70 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-71 to enable the CTC_HEAP variable change. **Note** This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.

Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Microsoft Windows

Note Before proceeding with the following steps, ensure that your system has a minimum of 1 GB of RAM. If your system does not have a minimum of 1 GB of RAM, contact the Cisco Technical Assistance Center (TAC).

Step 1 Close all open CTC sessions and browser windows.

Step 2 From the Microsoft Windows Start menu, choose **Control Panel > System.**

Step 3 In the System Properties window, click the **Advanced** tab.

Step 4 Click the **Environment Variables** button to open the Environment Variables window.

Step 5 Click the **New** button under the System variables field.

Step 6 Type `CTC_HEAP` in the Variable Name field.

Step 7 Type `512` in the Variable Value field, and then click the **OK** button to create the variable.

Step 8 Again, click the **New** button under the System variables field.

Step 9 Type `CTC_MAX_PERM_SIZE_HEAP` in the Variable Name field.

Step 10 Type `128` in the Variable Value field, and then click the **OK** button to create the variable.

Step 11 Click the **OK** button in the Environment Variables window to accept the changes.

Step 12 Click the **OK** button in the System Properties window to accept the changes.

Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris

Step 1 From the user shell window, kill any CTC sessions and browser applications.

Step 2 In the user shell window, set the environment variables to increase the heap size.

The following example shows how to set the environment variables in the C shell:

```
% setenv CTC_HEAP 512
% setenv CTC_MAX_PERM_SIZE_HEAP 128
```

1.10.3 Browser Stalls When Downloading CTC JAR Files from port

Symptom The browser stalls or hangs when downloading a CTC Java archive (JAR) file from the port.

Table 1-10 describes the potential cause of the symptom and the solution.

Table 1-10 Browser Stalls When Downloading JAR File from Port

Possible Problem	Solution
McAfee VirusScan software might be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later.	Disable the VirusScan Download Scan feature. See the "Disable the VirusScan Download Scan" procedure on page 1-72.

Disable the VirusScan Download Scan

Step 1 From the Microsoft Windows Start menu, choose **Programs > Network Associates > VirusScan Console**.

Step 2 Double-click the **VShield** icon listed in the VirusScan Console dialog box.

Step 3 Click **Configure** on the lower part of the Task Properties window.

Step 4 Click the **Download Scan** icon on the left of the System Scan Properties dialog box.

Step 5 Uncheck the **Enable Internet download scanning** check box.

Step 6 Click **Yes** when the warning message appears.

Step 7 Click **OK** on the System Scan Properties dialog box.

Step 8 Click **OK** on the Task Properties window.

Step 9 Close the McAfee VirusScan window.

1.10.4 CTC Does Not Launch

Symptom CTC does not launch; usually an error message appears before the login window appears.

Table 1-11 describes the potential cause of the symptom and the solution.

Table 1-11 CTC Does Not Launch

Possible Problem	Solution
The Netscape browser cache might point to an invalid directory.	Redirect the Netscape cache to a valid directory. See the "Redirect the Netscape Cache to a Valid Directory" procedure on page 1-72.

Redirect the Netscape Cache to a Valid Directory

Step 1 Launch Netscape.

Step 2 From the **Edit** menu, choose **Preferences**.

Step 3 In the Category column on the left side, expand **Advanced** and select the **Cache** tab.

Step 4 Change your disk cache folder to point to the cache file location.

The cache file location is usually C:\ProgramFiles\Netscape\Users*yourname*\cache. The *yourname* segment of the file location is often the same as the user name.

1.10.5 Sluggish CTC Operation or Login Problems

Symptom You experience sluggish CTC operation or have problems logging into CTC.

Table 1-12 describes the potential cause of the symptom and the solution.

Table 1-12 Sluggish CTC Operation or Login Problems

Possible Problem	Solution
The CTC cache file might be corrupted or might need to be replaced.	Delete the CTC cache file. This operation forces the ONS 15310-CL or ONS 15310-MA to download a new set of JAR files to your computer hard drive. See the "Delete the CTC Cache File Automatically" procedure on page 1-73 if you want to temporarily delete the cache stored from another CTC session, or the "Delete the CTC Cache File Manually" procedure on page 1-74 if you want to delete the Java archive (JAR) files associated with an older JRE version.
Insufficient heap memory allocation.	Increase the heap size if you are using CTC to manage more than 50 nodes concurrently. See the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Microsoft Windows" procedure on page 1-70 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-71. **Note** To avoid network performance issues, Cisco recommends managing a maximum of 50 nodes concurrently with CTC. To manage more than 50 nodes, Cisco recommends using Cisco Transport Manager (CTM). Cisco does not recommend running multiple CTC sessions when managing two or more large networks.

Delete the CTC Cache File Automatically

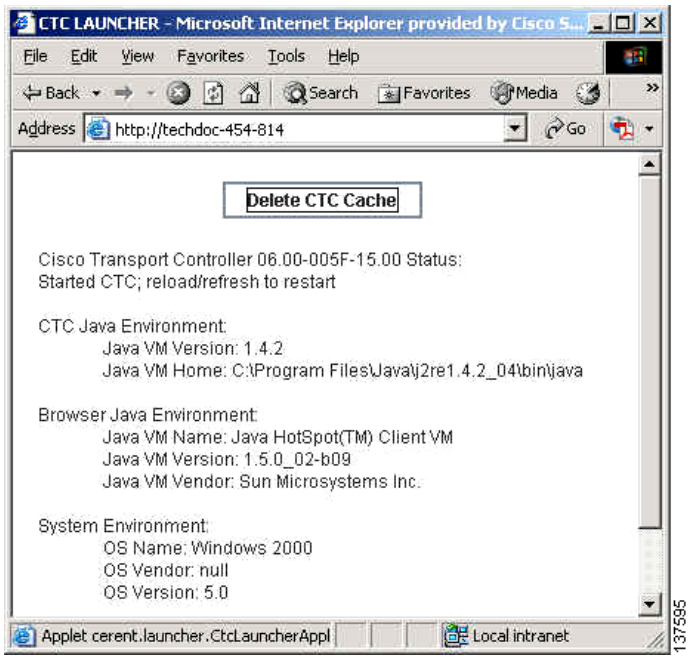
Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting the CTC cache might cause any CTC sessions running on this system to behave in an unexpected manner.

Step 1 Enter an ONS 15310-CL or ONS 15310-MA IP address in the browser URL field. The initial browser window shows a **Delete CTC Cache** button.

Step 2 Close all open CTC sessions and browser windows. The Microsoft Windows PC operating system does not allow you to delete files that are in use.

Step 3 Click **Delete CTC Cache** on the initial browser window to clear the CTC cache. Figure 1-10 shows the Delete CTC Cache window.

Figure 1-10 Deleting the CTC Cache



Delete the CTC Cache File Manually

Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting the CTC cache might cause any CTC running on this system to behave in an unexpected manner.

Step 1 To delete the JAR files manually, from the Microsoft Windows Start menu choose **Search > For Files or Folders**.

Step 2 Enter **ctc*.jar or cms*.jar** in the Search for Files or Folders Named field on the Search Results dialog box and click **Search Now**.

Step 3 Click the **Modified** column on the Search Results dialog box to find the JAR files that match the date when you downloaded the files from the port.

Step 4 Highlight the files and press the keyboard **Delete** key.

Step 5 Click **Yes** in the Confirm dialog box.

1.10.6 Node Icon is Gray on CTC Network View

Symptom The CTC network view shows one or more node icons as gray in color and without a node name.

Table 1-13 describes the potential causes of the symptom and the solutions.

Table 1-13 Node Icon is Gray on CTC Network View

Possible Problem	Solution
Different CTC releases are not recognizing each other. Usually accompanied by an INCOMPATIBLE-SW alarm.	Correct the core version build as described in the "1.10.8 Different CTC Releases Do Not Recognize Each Other" section on page 1-76.
A username/password mismatch. Usually accompanied by a NOT-AUTHENTICATED condition.	Correct the username and password as described in the "1.10.9 Username or Password Does Not Match the Port Information" section on page 1-77.
No IP connectivity between nodes. Usually accompanied by Ethernet-specific alarms.	Verify the Ethernet connections as described in the "Cisco Transport Controller Operation" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.
A lost DCC connection. Usually accompanied by a procedural error mismatch (EOC) alarm.	Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm on page 2-54.

1.10.7 Java Runtime Environment Incompatible

Symptom The CTC application does not run properly.

Table 1-14 describes the potential cause of the symptom and the solution.

Table 1-14 Java Runtime Environment Incompatible

Possible Problem	Solution
The compatible Java 2 JRE is not installed.	The Java 2 JRE contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. **Note** CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco software CD and on the Cisco ONS 15310-CL and ONS 15310-MA documentation CD. See the "Launch CTC to Correct the Core Version Build" procedure on page 1-76. **Note** If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with all of the releases that you are running. See Table 1-15 on page 1-76.

Note CTC will notify you if an older version JRE is running on your Microsoft Windows PC or UNIX workstation.

Launch CTC to Correct the Core Version Build

Step 1 Exit the current CTC session and completely close the browser.

Step 2 Start the browser.

Step 3 Type the node IP address of the node that reported the alarm. This can be the original IP address you logged in with or an IP address other than the original.

Step 4 Log into CTC. The browser downloads the JAR file from CTC.

1.10.8 Different CTC Releases Do Not Recognize Each Other

Symptom Different CTC releases on the same network do not recognize each other.

Table 1-15 describes the potential cause of the symptom and the solution.

Table 1-15 Different CTC Releases Do Not Recognize Each Other

Possible Problem	Solution
The software loaded on the connecting workstation and the software on the ONS 15310-CL or ONS 15310-MA are incompatible.	This occurs when the port software is upgraded but the Microsoft Windows PC has not yet upgraded the compatible CTC JAR file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version. See the "Launch CTC to Correct the Core Version Build" procedure on page 1-76. **Note** Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or earlier and then attempt to log into another ONS node in the network running a later CTC core version, the earlier version node does not recognize the new node. **Note** This situation is often accompanied by the INCOMPATIBLE-SW alarm.

Launch CTC to Correct the Core Version Build

Step 1 Exit the current CTC session and completely close the browser.

Step 2 Start the browser.

Step 3 In the Node Name field, type the ONS 15310-CL or ONS 15310-MA IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.

Step 4 Log into CTC. The browser downloads the JAR file from port.

1.10.9 Username or Password Does Not Match the Port Information

Symptom A mismatch often occurs concurrently with a NOT-AUTHENTICATED alarm.

Table 1-16 describes the potential causes of the symptom and the solutions.

Table 1-16 Username or Password Does Not Match the Port Information

Possible Problem	Solution
The username or password entered does not match the information stored in the port.	All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For initial login to the node, enter the CISCO15 user name in capital letters and click **Login** and use the password "otbu+1," which is case-sensitive. See the "Verify Correct Username and Password" procedure on page 1-77.
	If the node has been configured for Remote Authentication Dial In User Service (RADIUS) authentication, the username and password are verified against the RADIUS server database rather than the security information in the local node database. For more information about RADIUS security, refer to the "Security" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

Verify Correct Username and Password

Step 1 Ensure that your keyboard Caps Lock key is not turned on and affecting the case-sensitive entry of the username and password.

Step 2 Contact your system administrator to verify the username and password.

Step 3 Contact the Cisco TAC at http://www.cisco.com/tac or 1-800-553-2447 to have them enter your system and create a new user name and password.

1.10.10 Superuser Password Needs to Be Reset

Symptom The Superuser password has been lost or compromised.

Table 1-17 describes the potential cause of the symptom and the solution.

Table 1-17 No IP Connectivity Exists Between Nodes

Possible Problem	Solution
A security breach or record-keeping error has occurred.	Reset the node to the default Superuser UID and password combination using the lamp test button.

Reset the ONS 15310-CL or ONS 15310-MA Password

Note To complete this procedure, you must be on site and have IP connectivity to the node.

Step 1 At the ONS 15310-CL or ONS 15310-MA shelf, locate the recessed button labeled LAMP TEST on the front of the unit.

Step 2 Using a pen tip or something of similar size, press in and hold down the recessed button labelled LAMP TEST for five seconds.

Step 3 Release the LAMP TEST button for approximately two seconds.

Step 4 Again press and hold down the recessed button labeled LAMP TEST for five seconds.

Step 5 Again release the LAMP TEST button.

Step 6 Start a normal CTC session. At the login screen, CTC accepts the default username and password set when the system shipped. The default username is **CISCO15** and the password is **otbu+1**. CISCO15 has Superuser rights and privileges, which allow you to create a user name and assign a password.

Note Other existing usernames and passwords are not affected by the reset. The superuser reset applies only to the local node where the procedure is performed.

Step 7 If you need to create another user name and password, complete the following steps:

a. Click the **Provisioning** > **Security** tabs and click **Create**.

b. Fill in the fields with a new user name and password and assign a security level.

c. Click **OK**.

Note After new user names and passwords are set up, including at least one Superuser, log in as a newly created Superuser and delete the default CISCO15 username and otbu+1 password to ensure security is not compromised.

1.10.11 No IP Connectivity Exists Between Nodes

Symptom The nodes have a gray icon that is usually accompanied by alarms.

Table 1-18 describes the potential cause of the symptom and the solution.

Table 1-18 No IP Connectivity Exists Between Nodes

Possible Problem	Solution
Lost Ethernet connection	Usually, this condition is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in Chapter 8, "CTC Network Connectivity," of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

1.10.12 DCC Connection Lost

Symptom The node is usually accompanied by alarms and the nodes in the network view have a gray icon.

Table 1-19 describes the potential cause of the symptom and the solution.

Table 1-19 DCC Connection Lost

Possible Problem	Solution
A lost DCC connection	Usually, this condition is accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm on page 2-54.

1.10.13 "Path in Use" Error When Creating a Circuit

Symptom While creating a circuit, you get a "Path in Use" error that prevents you from completing the circuit creation.

Table 1-20 describes the potential cause of the symptom and the solution.

Table 1-20 "Path in Use" Error When Creating a Circuit

Possible Problem	Solution
Another user has already selected the same source port to create another circuit	CTC does not remove a card or port from the available list until a circuit is completely provisioned. If two users simultaneously select the same source port to create a circuit, the first user to complete circuit provisioning gets use of the port. The other user gets the "Path in Use" error. See the "Cancel the Circuit Creation and Start Over" procedure on page 1-79.

Cancel the Circuit Creation and Start Over

Step 1 Cancel the circuit creation:

a. Click **Cancel**.

b. Click **Back** until you return to the initial circuit creation window.

Step 2 Check the list of available ports. The previously selected port no longer appears in the available list because it is now part of a provisioned circuit.

Step 3 Select a different available port and begin the circuit creation process.

1.10.14 Calculate and Design IP Subnets

Symptom You cannot calculate or design IP subnets on the ONS 15310-CL or ONS 15310-MA.

Table 1-21 describes the potential cause of the symptom and the solution.

Table 1-21 Calculate and Design IP Subnets

Possible Problem	Solution
The IP capabilities of the ONS 15310-CL and ONS 15310-MA require specific calculations to properly design IP subnets.	Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/cgi-bin/Support/IpSubnet/subnets.pl. For information about ONS 15310-CL or ONS 15310-MA IP capability, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.

1.11 Circuits and Timing

This section provides solutions to circuit creation and reporting errors, as well as common timing reference errors and alarms.

1.11.1 Circuit Transitions to Partial Status

Symptom An automatic or manual transition of another state results in the OOS-PARTIAL state; at least one of the connections in the circuit is in IS-NR state and at least one other connection in the circuit is in IS,AINS, OOS,MT, or OOS_AINS state.

Table 1-22 describes the potential causes of the symptom and the solutions.

Table 1-22 Circuit in Partial Status

Possible Problem	Solution
During a manual transition, CTC cannot communicate with one of the nodes or one of the nodes is on a version of software that does not support the new state model.	Repeat the manual transition operation. If the Partial status persists, determine which node in the circuit is not changing to the desired state. See the "View the State of Circuit Nodes" procedure on page 1-81. Log onto the circuit node that did not change to the desired state and determine the version of software. Refer to the release-specific software upgrade guide for software upgrade procedures.
During an automatic transition, some path-level defects and/or alarms were detected on the circuit. One end of the circuit is not properly terminated.	Determine which node in the circuit is not changing to the desired state. Refer to the "View the State of Circuit Nodes" procedure on page 1-81. Log into the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures to clear alarms and change circuit configuration settings. Resolve and clear the defects and alarms on the circuit node and verify that the circuit transitions to the desired state.

View the State of Circuit Nodes

Step 1 Click the **Circuits** tab.

Step 2 From the Circuits tab list, select the circuit with the OOS-PARTIAL status condition.

Step 3 Click **Edit**. The Edit Circuit window appears.

Step 4 In the Edit Circuit window, click the **State** tab.

The State tab window lists the Node, CRS End A, CRS End B, and CRS State for each of the nodes in the circuit.

1.11.2 Circuits Remain in PARTIAL Status

Symptom Circuits remain in the PARTIAL status.

Table 1-23 describes the potential cause of the symptom and the solution.

Table 1-23 Circuits Remain in PARTIAL Status

Possible Problem	Solution
The MAC address changed.	Repair the circuits. Refer to the "Manage Circuits" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for instructions.

1.11.3 AIS-V on Unused 15310-CL-CTX Card VT Circuits

Symptom An incomplete circuit path causes an alarm indications signal (AIS).

Table 1-24 describes the potential cause of the symptom and the solution.

Table 1-24 AIS-V on Unused 15310-CL-CTX Card VT Circuits

Possible Problem	Solution
The port on the reporting node is in-service but a node upstream on the circuit does not have an OC-N port in service.	An AIS-V indicates that an upstream failure occurred at the VT layer. AIS-V alarms also occur on VT circuits that are not carrying traffic and on stranded bandwidth. Perform the "Clear AIS-V on Unused Controller Card VT Circuits" procedure on page 1-82.

Clear AIS-V on Unused Controller Card VT Circuits

Step 1 Determine the affected port.

Step 2 Record the node ID, slot number, port number, and VT number.

Step 3 Create a unidirectional VT circuit from the affected port back to itself, such as Source node/Slot 2/Port 2/VT 13 cross connected to Source node/Slot 2/Port 2/VT 13.

Step 4 Uncheck the Bidirectional check box in the circuit creation window.

Step 5 Give the unidirectional VT circuit an easily recognizable name, such as DeleteMe.

Step 6 Display the controller card (15310-CL-CTX or CTX2500) in CTC card view. Click the **Maintenance > DS1** tabs.

Step 7 Locate the VT that is reporting the alarm (for example, DS3 #2, DS1 #13).

Step 8 From the Loopback Type list, choose **Facility** and click **Apply**.

Step 9 Click **Circuits**.

Step 10 Find the one-way circuit you created in Step 3. Select the circuit and click **Delete**.

Step 11 Click **Yes** in the Delete Confirmation dialog box.

Step 12 In node view, double-click the controller card (15310-CL-CTX or CTX2500). The card view appears.

Step 13 Click the **Maintenance > DS1** tabs.

Step 14 Locate the VT in the Facility Loopback list.

Step 15 From the Loopback Type list, choose **None** and then click **Apply**.

Step 16 Click the **Alarm** tab and verify that the AIS-V alarms have cleared.

Step 17 Repeat this procedure for all the AIS-V alarms on the controller.

1.11.4 Circuit Creation Error with VT1.5 Circuit

Symptom You might receive an "Error while finishing circuit creation. Unable to provision circuit. Unable to create connection object at *node-name*" message when trying to create a VT1.5 circuit in CTC.

Table 1-25 describes the potential causes of the symptom and the solutions.

Table 1-25 Circuit Creation Error with VT1.5 Circuit

Possible Problem	Solution
You might have run out of bandwidth on the VT cross-connect matrix at the node indicated in the error message.	The ONS 15310-CL matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects. The ONS 15310-MA capacity is 1,064.

1.11.5 OC-3 and DCC Limitations

Symptom There are limitations to OC-3 and DCC usage.

Table 1-26 describes the potential cause of the symptom and the solution.

Table 1-26 OC-3 and DCC Limitations

Possible Problem	Solution
OC-3 and DCC have limitations for the system.	For an explanation of OC-3 and DCC limitations, refer to the "DCC Tunnels" section in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

1.11.6 ONS 15310-CL or ONS 15310-MA Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

Table 1-27 describes the potential causes of the symptom and the solutions.

Table 1-27 ONS 15310-CL or ONS 15310-MA Switches Timing Reference

Possible Problem	Solution
The optical or building integrated timing supply (BITS) input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source.	The node internal clock operates at a Stratum 3 level of accuracy. This gives the node a free-running synchronization accuracy of +/–4.6 ppm and a holdover stability of less than 255 slips in the first 24 hours or 3.7 x 10^{-7} per day, including temperature. Node free-running synchronization relies on the Stratum 3 internal clock. Use a higher quality Stratum 1 or Stratum 2 timing source. This results in fewer timing slips than a lower quality Stratum 3 timing source.
The optical or BITS input is not functioning.	
Synchronization status message (SSM) is set to Don't Use for Synchronization (DUS).	
SSM indicates a Stratum 3 or lower clock quality.	
The input frequency is off by more than 15 ppm.	
The input clock wanders and has more than three slips in 30 seconds.	
A bad timing reference existed for at least two minutes.	

1.11.7 Holdover Synchronization Alarm

Symptom The clock is running at a different frequency than normal and the holdover synchronization (HLDOVRSYNC) alarm appears.

Table 1-28 describes the potential cause of the symptom and the solution.

Table 1-28 Holdover Synchronization Alarm

Possible Problem	Solution
The last reference input has failed.	The clock is running at the frequency of the last valid reference input. This alarm is raised when the last reference input fails. See the "HLDOVRSYNC" alarm on page 2-79 for a detailed description of this alarm. **Note** The ONS 15310-CL and ONS 15310-MA support holdover timing per Telcordia GR-4436 when provisioned for external (BITS) timing.

1.11.8 Free-Running Synchronization Mode

Symptom The clock is running at a different frequency than normal and the free-running synchronization(2.7.98 FRNGSYNC) alarm appears.

Table 1-29 describes the potential cause of the symptom and the solution.

Table 1-29 Free-Running Synchronization Mode

Possible Problem	Solution
No reliable reference input is available.	The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the "FRNGSYNC" alarm on page 2-72 for a detailed description of this alarm.

1.11.9 Daisy-Chained BITS Not Functioning

Symptom You are unable to daisy-chain the BITS.

Table 1-30 describes the potential cause of the symptom and the solution.

Table 1-30 Daisy-Chained BITS Not Functioning

Possible Problem	Solution
Daisy-chaining BITS is not supported on the system.	Daisy-chaining BITS causes additional wander buildup in the network and is therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each node.

1.11.10 Blinking STAT LED after Installing a Card

Symptom After installing a card, the STAT LED blinks continuously for more than 60 seconds.

Table 1-31 describes the potential cause of the symptom and the solution.

Table 1-31 Blinking STAT LED on Installed Card

Possible Problem	Solution
The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics.	The blinking STAT LED indicates that POST diagnostics are being performed. If the LED continues to blink more than 60 seconds, the card has failed the POST diagnostics test and has failed to boot. If the card has truly failed, an EQPT-BOOT alarm is raised against the slot number with an "Equipment Fails To Boot" description. Check the alarm tab for this alarm to appear for the slot where the card is installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card.

1.12 Fiber and Cabling

This section explains problems typically caused by cabling connectivity errors. It also includes instructions for crimping CAT-5 cable and lists the optical fiber connectivity levels.

1.12.1 Bit Errors Appear for a Traffic Card

Symptom A traffic card has multiple bit errors.

Table 1-32 describes the potential cause of the symptom and the solution.

Table 1-32 Bit Errors Appear for a Line Card

Possible Problem	Solution
Faulty cabling or low optical-line levels.	Troubleshoot cabling problems using the "1.1 Network Troubleshooting Tests" section on page 1-2. Troubleshoot low optical levels using procedures in the "1.12.2 Faulty Fiber-Optic Connections" section on page 1-86. **Note** Bit errors on line (traffic) ports usually originate from cabling problems or low optical-line levels. The errors can be caused by synchronization problems, especially if pointer justification (PJ) errors are reported. Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the node.

1.12.2 Faulty Fiber-Optic Connections

Symptom A line card has multiple SONET alarms and/or signal errors.

Table 1-33 describes the potential causes of the symptom and the solutions.

Table 1-33 Faulty Fiber-Optic Connections

Possible Problem	Solution
Faulty fiber-optic connections.	Faulty fiber-optic connections can be the source of SONET alarms and signal errors. See the "Verify Fiber-Optic Connections" procedure on page 1-87.
Faulty CAT-5 cables.	Faulty CAT-5 cables can be the source of SONET alarms and signal errors. See the "1.12.2.1 Crimp Replacement LAN Cables" procedure on page 1-88.

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm may pose an eye hazard.** Statement 1056

Warning **Class 1 laser product.** Statement 1008

Warning **Laser radiation presents an invisible hazard, so personnel should avoid exposure to the laser beam. Personnel must be qualified in laser safety procedures and must use proper eye protection before working on this equipment.** Statement 300

Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects to the ONS 15310-CL or ONS 15310-MA Small form-factor Pluggable (SFP).

SM or SM Fiber should be printed on the fiber span cable. ONS 15310-CL and ONS 15310-MA ports do not use multimode fiber.

Step 2 Ensure that the connector keys on the SC fiber connector are properly aligned and locked.

Step 3 Check that the single-mode fiber power level is within the specified range:

a. Remove the Rx end of the suspect fiber.

b. Connect the receive end of the suspect fiber to a fiber-optic power meter, such as a GN Nettest LP-5000.

c. Determine the power level of fiber with the fiber-optic power meter.

d. Verify that the power meter is set to the appropriate wavelength for the optical port being tested (either 1310 nm or 1550 nm).

e. Verify that the power level falls within the range specified for the card; refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for information.

Step 4 If the power level falls below the specified range:

a. Clean or replace the fiber patchcords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*. If possible, do this for the OC-N port you are working on and the far-end ONS 15310-CL or ONS 15310-MA.

b. Clean the optical connectors on the port. Clean the connectors according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*. If possible, do this for the card you are working on and the far-end node.

c. If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):

- Excessive fiber distance—Single-mode fiber attenuates at approximately 0.5 dB/km.
- Excessive number or fiber connectors—Connectors take approximately 0.5 dB each.
- Excessive number of fiber splices—Splices take approximately 0.5 dB each.

Note These are typical attenuation values. Refer to the specific product documentation for the actual values or use an optical time domain reflectometer (OTDR) to establish precise link loss and budget requirements.

Step 5 If no power level shows on the fiber, the fiber is bad or the transmitter on the optical port failed. Complete the following steps:

a. Check that the Tx and Rx fibers are not reversed. LOS and EOC alarms normally accompany reversed Tx and Rx fibers. Switching reversed Tx and Rx fibers clears the alarms and restores the signal.

b. Clean or replace the fiber patchcords. Clean the fiber according to site practice or, if none exists, follow the procedure in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*. If possible, do this for the card you are working on and the far-end card.

c. Retest the fiber power level.

Tip Most fiber has text printed on only one of the two fiber strands. Use this to identify which fiber is connected to Tx and which fiber is connected to Rx.

1.12.2.1 Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the system. Use #22 or #24 AWG shielded wire with RJ-45 connectors and a crimping tool.

Use a cross-over cable when connecting an ONS 15310-CL or ONS 15310-MA to a hub, LAN modem, or switch, and use a LAN cable when connecting a node to a router or workstation.

Figure 1-11 shows the layout of an RJ-45 connector.

Figure 1-11 RJ-45 Pin Numbers

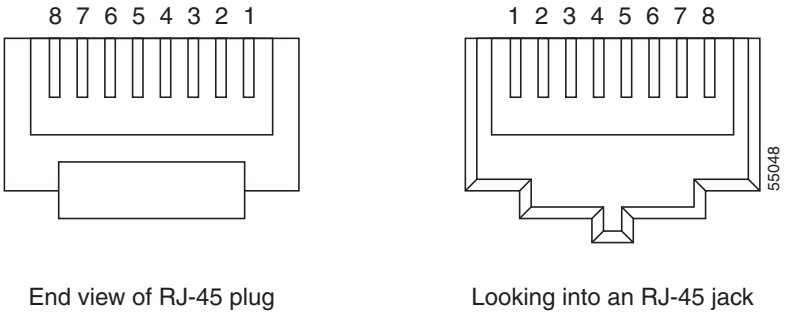


Figure 1-12 shows the layout of a LAN cable.

Figure 1-12 LAN Cable Layout

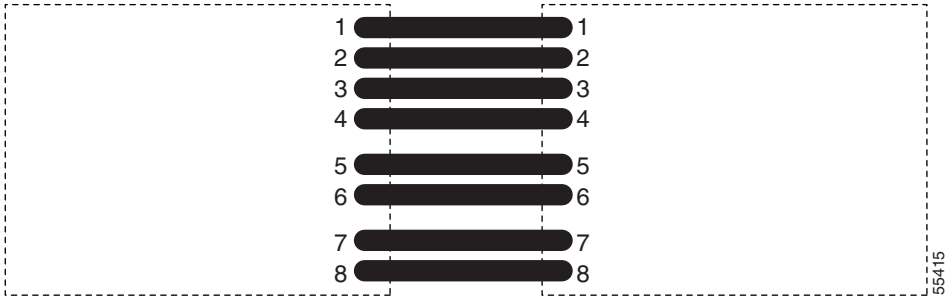


Table 1-34 shows LAN cable pinouts.

Table 1-34 LAN Cable Pinout

Pin	Color	Pair	Name	Pin
1	White/orange	2	Transmit Data +	1
2	Orange	2	Transmit Data -	2
3	White/green	3	Receive Data +	3
4	Blue	1	—	4
5	White/blue	1	—	5
6	Green	3	Receive Data –	6
7	White/brown	4	—	7
8	Brown	4	—	8

Figure 1-13 shows the layout of a cross-over cable.

Figure 1-13 Cross-Over Cable Layout

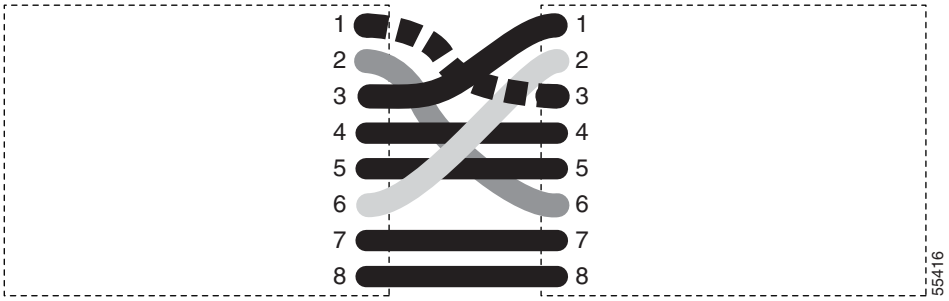


Table 1-35 shows cross-over cable pinouts.

Table 1-35 Cross-Over Cable Pinout

Pin	Color	Pair	Name	Pin
1	White/orange	2	Transmit Data +	3
2	Orange	2	Transmit Data –	6
3	White/green	3	Receive Data +	1

Table 1-35 Cross-Over Cable Pinout (continued)

Pin	Color	Pair	Name	Pin
4	Blue	1	—	4
5	White/blue	1	—	5
6	Green	3	Receive Data –	2
7	White/brown	4	—	7
8	Brown	4	—	8

Note Odd-numbered pins always connect to a white wire with a colored stripe.

1.13 Power and LED Tests

This section provides symptoms and solutions for power supply problems, power consumption, and LED indicators.

1.13.1 Power Supply Problems

Symptom Loss of power or low voltage, resulting in a loss of traffic and causing the LCD clock to reset to the default date and time.

Table 1-36 describes the potential causes of the symptom and the solutions.

Table 1-36 Power Supply Problems

Possible Problem	Solution
Loss of power or low voltage	See Chapter 2, "Alarm Troubleshooting," for information about specific power alarms. Procedures for installing power supply and cables are located in the "Install Hardware" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*. Power supplies may be disconnected by reversing the appropriate procedure (for AC or DC power). **Note** The ONS 15310-CL and ONS 15310-MA require a constant source of DC power to properly function. Input power is –48 VDC. Power requirements range from –42 VDC to –57 VDC. **Note** A newly installed ONS 15310-CL or ONS 15310-MA that is not properly connected to its power supply does not operate. Power problems can be confined to a specific node or can affect several pieces of equipment on the site. **Note** A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the node to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General** tabs and change the Date and Time fields.
Improperly connected power supply	

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Caution Operations that interrupt power supply or short the power connections to the system are service-affecting.

1.13.2 Power Consumption for Node and Cards

Symptom You are unable to power up a node or the cards in a node.

Table 1-37 describes the potential cause of the symptom and the solution.

Table 1-37 Power Consumption for Node and Cards

Possible Problem	Solution
Improper power supply.	Refer to power information in the "Install Hardware" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

1.13.3 Lamp Tests for Card LEDs

Symptom Optical (OC-N) ports LEDs do not light, or you are unsure whether the LEDs are working properly.

The LED lamp test determines whether card-level LEDs are operational. For optical ports, this test also causes port-level LEDs to turn on. For Ethernet cards, only card-level LEDs light. For these cards, port-level LEDs can be compared to the given guidelines to determine whether they are working correctly.

Optical port LEDs light during the lamp test. Ethernet cards only illuminate card-level LEDs during the test. Table 1-38 describes the possible problem and the solution for optical ports.

Table 1-38 Lamp Test for Optical and Electrical Card LEDs

Possible Problem	Solution
Faulty optical port LED	A lamp test verifies that all the port LEDs work. Run this diagnostic test as part of the initial system turn-up, a periodic maintenance routine, or any time you question whether an LED is in working order. Complete the "Verify Card LED Operation" procedure on page 1-92.

Verify Card LED Operation

Step 1 In CTC, click the **Maintenance > Diagnostic** tabs.

Step 2 Click **Lamp Test**.

Step 3 Watch to make sure all the port LEDs illuminate as previously noted for several seconds.

Step 4 Click **OK** on the Lamp Test Run dialog box.

With the exceptions previously described, if an OC-N or DS-N LED does not light up, the LED is faulty. Return the defective card to Cisco through the RMA process. Contact Cisco TAC at http://www.cisco.com/tac or 1-800-553-2447.

1.13.4 Retrieve Tech Support Logs Button

When you click the Retrieve Tech Support Logs button in the Diagnostics tab of the Maintenance window, CTC retrieves system data that a Retrieve or higher level user can off-load to a local directory and sent to Technical Support for troubleshooting purposes. The diagnostics file is in machine language and is not human-readable, but can be used by Cisco Technical Support for problem analysis. Complete the following procedure to off-load the diagnostics file.

Note In addition to the machine-readable diagnostics file, the ONS 15454 stores an audit trail of all system events such as user log-ins, remote log-ins, configuration, and changes. This audit trail is considered a record-keeping feature rather than a troubleshooting feature. Information about the feature is located in the "Maintain the Node" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Off-Load the Diagnostics File

Note The diagnostics operation is performed at a shelf level. Only single-node-related diagnostic information can be downloaded at a time.

The diagnostic files retrieved by CTC depends on the user privilege levels. Table 1-39 lists the user privilege levels and the diagnostic retrieval operations they can perform.

Table 1-39 Diagnostic Files Retrieved Based on User Privilege

User Privilege Level	Diagnostic File Retrieval Operation
Retrieve	• Export the unfiltered alarm table contents • Export the unfiltered conditions table contents • Export the unfiltered history table contents • Export the inventory table contents • CTC Dump Diagnostics log
Maintenance	• All Retrieve level access operations • Save the node database
Provisioning	• All Maintenance level access operations • Retrieve and save the node-level diagnostics report[1] • Export the audit table contents[2]
Superuser	• All Provisioning level access operations • Retrieve and save the node-level diagnostics report • Export the audit table contents

1. If secure mode is not set on the node.
2. If the NODE.security.grantPermission.RetrieveAuditLog NE Default is set to “Provisioning.”

Step 1 In the node view, click the **Maintenance > Diagnostic** tabs.

Step 2 Click **Retrieve Tech Support Logs** in the Controller area.

Step 3 In the Select a Filename for the Tech Support Logs Zip Archive dialog box, add the diagnostics file name in the format **TechSupportLogs_**<*node_name*>**.zip** by default. Substitute the last 20 alphanumeric characters of the node name for <*node_name*>. Navigate to the directory (local or network) where you want to save the file.

A message appears asking you if you want to overwrite any existing disgnostics file in the selected directory.

Step 4 Click **Save**.

CTC performs the diagnostic tasks and writes the diagnostic files in a folder named TechSupportLogs_<*node_name*> under the location selected in Step 3. After all the diagnostic files are written to the TechSupportLogs_<*node_name*> folder, CTC archives the retrieved diagnostic files as TechSupportLogs_<*node_name*>.zip. CTC deletes the TechSupportLogs_<*node_name*> folder after the archiving process is successfully completed. CTC retains this folder if the archiving process fails. The retrieved diagnostic files can be accessed in the TechSupportLogs_<*node_name*> folder.

A progress bar indicates the percentage of the file that is being saved. The Save Tech Support Logs Completed dialog box appears when the file is saved. CTC logs any error during the retrieval and archiving of diagnostics file to the CTC Alerts Log.

Table 1-40 lists the diagnostic files retrieved by CTC.

Table 1-40 List of Diagnostic Files

Diagnostic File	Diagnostic File Content
AlarmTableLog.html	Alarm Table export
HistoryTableLog.html	Alarm Table export
ConditionsTableLog.html	Conditions Table export
InventoryTableLog.html	Inventory Table export
AuditTableLog.html	Audit Table export
CTCDumpDiagLog.txt	Audit Table export
NodeDiagnostics.bin	NodeDiagnostics.gz
OBFLDiagnostics.bin	OBFLDiagnostics.bin
NodeDatabaseBackup.bin	Database backup
TechSupportLogs_<*node_name*>.zip	Zip archive of all the diagnostics file

Step 5 Click **OK**.

CHAPTER 2

Alarm Troubleshooting

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15310-CL and ONS 15310-MA alarm and condition. Tables 2-1 through 2-5 list the alarms of both platforms, organized by severity. Table 2-6 on page 2-6 provides a list of alarms organized alphabetically. Table 2-7 gives definitions of all ONS 15310-CL and ONS 15310-MA alarm logical objects, which are the basis of the alarm profile list in Table 2-8 on page 2-12. For a comprehensive list of all conditions, refer to the *Cisco SONET TL1 Command Guide*. For further information about Transaction Language One (TL1), refer to the *Cisco ONS SONET TL1 Reference Guide*.

An alarm's troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and the TL1 version of that alarm. If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call the Cisco Technical Assistance Center (1-800-553-2447).

More information about alarm profile information modification and downloads is located in the "Manage Alarms" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

2.1 Alarm Index by Default Severity

The following tables group alarms and conditions by their default severities in the ONS 15310-CL and ONS 15310-MA systems. These severities are the same whether they are reported in the CTC Alarms window severity (SEV) column or in TL1.

Note The CTC default alarm profile contains some alarms or conditions that are not currently implemented but are reserved for future use.

Note The CTC default alarm profile in some cases contains two severities for one alarm (for example, Major/Minor [MJ/MN]). The default severity comes first (in this example, MJ), but the alarm can be demoted to the second severity in the presence of a higher-ranking alarm. This is in accordance with Telcordia GR-474-CORE.

2.1.1 Critical Alarms (CR)

Table 2-1 alphabetically lists ONS 15310-CL and ONS 15310-MA Critical (CR) alarms.

Table 2-1 ONS 15310-CL and ONS 15310-MA Critical Alarm List

AUTOLSROFF (OCN)	LINK-KEEPALIVE (ML100T)	MEA (PPM)
BKUPMEMP (EQPT)	LOA (VCG)	MFGMEM (BPLANE)
COMIOXC (EQPT)	LOF (DS3)	MFGMEM (FAN)
CONTBUS-DISABLED (EQPT)	LOF (EC1)	MFGMEM (PPM)
CTNEQPT-PBPROT (EQPT)	LOF (OCN)	PLM-P (STSMON)
CTNEQPT-PBWORK (EQPT)	LOF (STSTRM)	PLM-P (STSTRM)
ENCAP-MISMATCH-P (STSTRM)	LOM (STSMON)	SQM (STSTRM)
EQPT (EQPT)	LOM (STSTRM)	SWMTXMOD-PROT (EQPT)
EQPT (PPM)	LOP-P (STSMON)	SWMTXMOD-WORK (EQPT)
EQPT-MISS (FAN)	LOP-P (STSTRM)	TIM (OCN)
FAN (FAN)	LOS (DS3)	TIM-P (STSTRM)
HITEMP (NE)	LOS (EC1)	TIM-S (EC1)
I-HITEMP (NE)	LOS (OCN)	TIM-S (OCN)
IMPROPRMVL (EQPT)	MEA (EQPT)	UNEQ-P (STSMON)
IMPROPRMVL (PPM)	MEA (FAN)	UNEQ-P (STSTRM)

2.1.2 Major Alarms (MJ)

Table 2-2 alphabetically lists ONS 15310-CL and ONS 15310-MA Major (MJ) alarms.

Table 2-2 ONS 15310-CL and ONS 15310-MA Major Alarm List

APSCNMIS (OCN)	GFP-CSF (ML100T)	PLM-V (VT-MON)
BAT-FAIL (PWR)	GFP-LFD (CE100T)	PLM-V (VT-TERM)
BLSROSYNC (OCN)	GFP-LFD (CEMR)	PORT-MISMATCH (CEMR)
CARLOSS (CE100T)	GFP-LFD (ML100T)	PRC-DUPID (OCN)
CARLOSS (CEMR)	GFP-UP-MISMATCH (CE100T)	SHELF-COMM-FAIL (SHELF)
CARLOSS (EQPT)	GFP-UP-MISMATCH (CEMR)	SQM (VT-TERM)
CARLOSS (ML100T)	GFP-UP-MISMATCH (ML100T)	SYNCPRI (NE-SREF)
DATA-CRC (CE100T)	INVMACADR (BPLANE)	SYSBOOT (NE)

Table 2-2 ONS 15310-CL and ONS 15310-MA Major Alarm List (continued)

DATA-CRC (ML100T)	LOF (DS1)	TIM-V (VT-MON)
DUP-SHELF-ID (SHELF)	LOM (VT-TERM)	TIM-V (VT-TERM)
EHIBATVG (PWR)	LOP-V (VT-MON)	TPTFAIL (CE100T)
ELWBATVG (PWR)	LOP-V (VT-TERM)	TPTFAIL (CEMR)
FANDEGRADE (FAN)	LOS (DS1)	TPTFAIL (ML100T)
GFP-CSF (CE100T)	MEA (SHELF)	UNEQ-V (VT-MON)
GFP-CSF (CEMR)	MEM-GONE (EQPT)	UNEQ-V (VT-TERM)

2.1.3 Minor Alarms (MN)

Table 2-3 alphabetically lists ONS 15310-CL and ONS 15310-MA Minor (MN) alarms.

Table 2-3 ONS 15310-CL and ONS 15310-MA Minor Alarm List

APSB (OCN)	FEPRLF (OCN)	LO-TXPOWER (OCN)
APSCDFLTK (OCN)	FP-LINK-LOSS (EQPT)	LO-TXPOWER (PPM)
APSCINCON (OCN)	HELLO (OCN)	MATECLK (EQPT)
APSCM (OCN)	HI-LASERBIAS (OCN)	MEM-LOW (EQPT)
APSIMP (OCN)	HI-LASERBIAS (PPM)	PROTNA (EQPT)
APS-INV-PRIM (OCN)	HI-LASERTEMP (OCN)	PROV-MISMATCH (PPM)
APSMM (OCN)	HI-LASERTEMP (PPM)	PWR-FAIL-A (EQPT)
APS-PRIM-SEC-MISM (OCN)	HI-RXPOWER (OCN)	PWR-FAIL-B (EQPT)
AUTORESET (EQPT)	HITEMP (EQPT)	ROUTE-OVERFLOW (NSA)
CONTBUS-CLK-A (EQPT)	HI-TXPOWER (OCN)	SFTWDOWN (EQPT)
CONTBUS-CLK-B (EQPT)	HI-TXPOWER (PPM)	SNTP-HOST (NE)
CONTBUS-IO-A (EQPT)	ISIS-ADJ-FAIL (OCN)	SSM-FAIL (BITS)
CONTBUS-IO-B (EQPT)	LASEREOL (OCN)	SSM-FAIL (DS1)
DATAFLT (NE)	LOF (BITS)	SSM-FAIL (OCN)
DUP-IPADDR (NE)	LO-LASERBIAS (OCN)	SYNCPRI (EXT-SREF)
DUP-NODENAME (NE)	LO-LASERBIAS (PPM)	SYNCSEC (EXT-SREF)
EOC (OCN)	LO-LASERTEMP (OCN)	SYNCSEC (NE-SREF)
EOC-L (OCN)	LO-LASERTEMP (PPM)	SYNCTHIRD (EXT-SREF)
ERROR-CONFIG (EQPT)	LO-RXPOWER (OCN)	SYNCTHIRD (NE-SREF)
EXCCOL (EQPT)	LOS (BITS)	TIM-P (STSMON)
EXT (ENVALRM)	LOS (FUDC)	—

2.1.4 Not Alarmed Conditions

Table 2-4 alphabetically lists ONS 15310-CL and ONS 15310-MA Not Alarmed (NA) conditions.

Table 2-4 ONS 15310-CL and ONS 15310-MA NA Conditions List

ALS (OCN)	INHSWWKG (EQPT)	SF-P (STSTRM)
APC-END (NE)	INTRUSION-PSWD (NE)	SF-V (VT-MON)
APS-PRIM-FAC (OCN)	IOSCFGCOPY (EQPT)	SF-V (VT-TERM)
AS-CMD (BPLANE)	KB-PASSTHR (OCN)	SSM-DUS (BITS)
AS-CMD (CE100T)	LCAS-CRC (STSTRM)	SSM-DUS (DS1)
AS-CMD (CEMR)	LCAS-CRC (VT-TERM)	SSM-DUS (OCN)
AS-CMD (DS1)	LCAS-RX-DNU (STSTRM)	SSM-LNC (BITS)
AS-CMD (DS3)	LCAS-RX-DNU (VT-TERM)	SSM-LNC (NE-SREF)
AS-CMD (EC1)	LCAS-RX-FAIL (STSTRM)	SSM-LNC (OCN)
AS-CMD (EQPT)	LCAS-RX-FAIL (VT-TERM)	SSM-OFF (BITS)
AS-CMD (ML100T)	LCAS-RX-GRP-ERR (STSTRM)	SSM-OFF (DS1)
AS-CMD (NE)	LCAS-RX-GRP-ERR (VT-TERM)	SSM-OFF (OCN)
AS-CMD (OCN)	LCAS-TX-ADD (STSTRM)	SSM-PRC (BITS)
AS-CMD (PPM)	LCAS-TX-ADD (VT-TERM)	SSM-PRC (NE-SREF)
AS-CMD (PWR)	LCAS-TX-DNU (STSTRM)	SSM-PRC (OCN)
AS-CMD (SHELF)	LCAS-TX-DNU (VT-TERM)	SSM-PRS (BITS)
AS-MT (CE100T)	LKOUTPR-S (OCN)	SSM-PRS (DS1)
AS-MT (CEMR)	LOCKOUT-REQ (OCN)	SSM-PRS (NE-SREF)
AS-MT (DS1)	LOCKOUT-REQ (STSMON)	SSM-PRS (OCN)
AS-MT (DS3)	LOCKOUT-REQ (VT-MON)	SSM-RES (BITS)
AS-MT (EC1)	LPBKCRS (STSMON)	SSM-RES (DS1)
AS-MT (EQPT)	LPBKCRS (STSTRM)	SSM-RES (NE-SREF)
AS-MT (ML100T)	LPBKDS1FE-CMD (DS1)	SSM-RES (OCN)
AS-MT (OCN)	LPBKDS3FEAC (DS3)	SSM-SDH-TN (BITS)
AS-MT (PPM)	LPBKDS3FEAC-CMD (DS3)	SSM-SDH-TN (NE-SREF)
AS-MT (SHELF)	LPBKFACILITY (CE100T)	SSM-SDH-TN (OCN)
AS-MT-OOG (STSTRM)	LPBKFACILITY (CEMR)	SSM-SETS (BITS)
AS-MT-OOG (VT-TERM)	LPBKFACILITY (DS1)	SSM-SETS (NE-SREF)
AUD-LOG-LOSS (NE)	LPBKFACILITY (DS3)	SSM-SETS (OCN)
AUD-LOG-LOW (NE)	LPBKFACILITY (EC1)	SSM-SMC (BITS)
AUTOSW-LOP (STSMON)	LPBKFACILITY (OCN)	SSM-SMC (DS1)
AUTOSW-LOP (VT-MON)	LPBKTERMINAL (CE100T)	SSM-SMC (NE-SREF)
AUTOSW-PDI (STSMON)	LPBKTERMINAL (CEMR)	SSM-SMC (OCN)
AUTOSW-PDI (VT-MON)	LPBKTERMINAL (DS1)	SSM-ST2 (BITS)

Table 2-4 ONS 15310-CL and ONS 15310-MA NA Conditions List (continued)

AUTOSW-SDBER (STSMON)	LPBKTERMINAL (DS3)	SSM-ST2 (DS1)
AUTOSW-SDBER (VT-MON)	LPBKTERMINAL (EC1)	SSM-ST2 (NE-SREF)
AUTOSW-SFBER (STSMON)	LPBKTERMINAL (OCN)	SSM-ST2 (OCN)
AUTOSW-SFBER (VT-MON)	MAN-REQ (STSMON)	SSM-ST3 (BITS)
AUTOSW-UNEQ (STSMON)	MAN-REQ (VT-MON)	SSM-ST3 (DS1)
AUTOSW-UNEQ (VT-MON)	MANRESET (EQPT)	SSM-ST3 (NE-SREF)
CLDRESTART (EQPT)	MANSWTOINT (NE-SREF)	SSM-ST3 (OCN)
DS3-MISM (DS3)	MANSWTOPRI (EXT-SREF)	SSM-ST3E (BITS)
ETH-LINKLOSS (NE)	MANSWTOPRI (NE-SREF)	SSM-ST3E (DS1)
FAILTOSW (OCN)	MANSWTOSEC (EXT-SREF)	SSM-ST3E (NE-SREF)
FAILTOSW-PATH (STSMON)	MANSWTOSEC (NE-SREF)	SSM-ST3E (OCN)
FAILTOSW-PATH (VT-MON)	MANSWTOTHIRD (EXT-SREF)	SSM-ST4 (BITS)
FE-AIS (DS3)	MANSWTOTHIRD (NE-SREF)	SSM-ST4 (DS1)
FE-DS1-MULTLOS (DS3)	MANUAL-REQ-SPAN (OCN)	SSM-ST4 (NE-SREF)
FE-DS1-NSA (DS3)	NO-CONFIG (EQPT)	SSM-ST4 (OCN)
FE-DS1-SA (DS3)	OOU-TPT (STSTRM)	SSM-STU (BITS)
FE-DS1-SNGLLOS (DS3)	OOU-TPT (VT-TERM)	SSM-STU (DS1)
FE-DS3-NSA (DS3)	OPEN-SLOT (EQPT)	SSM-STU (NE-SREF)
FE-DS3-SA (DS3)	PDI-P (STSMON)	SSM-STU (OCN)
FE-EQPT-NSA (DS3)	PDI-P (STSTRM)	SSM-TNC (BITS)
FE-FRCDWKSWBK-SPAN (OCN)	RAI (DS1)	SSM-TNC (NE-SREF)
FE-FRCDWKSWPR-SPAN (OCN)	RAI (DS3)	SSM-TNC (OCN)
FE-IDLE (DS3)	ROLL (STSMON)	SW-MISMATCH (EQPT)
FE-LOCKOUTOFPR-SPAN (OCN)	ROLL (STSTRM)	SWTOPRI (EXT-SREF)
FE-LOF (DS3)	ROLL (VT-MON)	SWTOPRI (NE-SREF)
FE-LOS (DS3)	ROLL (VT-TERM)	SWTOSEC (EXT-SREF)
FE-MANWKSWBK-SPAN (OCN)	ROLL-PEND (STSMON)	SWTOSEC (NE-SREF)
FE-MANWKSWPR-SPAN (OCN)	ROLL-PEND (VT-MON)	SWTOTHIRD (EXT-SREF)
FORCED-REQ (STSMON)	ROLL-PEND (VT-TERM)	SWTOTHIRD (NE-SREF)
FORCED-REQ (VT-MON)	RPR-PASSTHR (RPRIF)	SYNC-FREQ (BITS)
FORCED-REQ-SPAN (OCN)	RPRW (ML100T)	SYNC-FREQ (DS1)
FRCDSWTOINT (NE-SREF)	RUNCFG-SAVENEED (EQPT)	SYNC-FREQ (OCN)
FRCDSWTOPRI (EXT-SREF)	SD (DS1)	TX-IDLE (DS1)
FRCDSWTOPRI (NE-SREF)	SD (DS3)	TX-RAI (DS1)
FRCDSWTOSEC (EXT-SREF)	SD-L (EC1)	TX-RAI (DS3)
FRCDSWTOSEC (NE-SREF)	SD-L (OCN)	VCG-DEG (VCG)
FRCDSWTOTHIRD (EXT-SREF)	SD-P (STSMON)	VCG-DOWN (VCG)

Table 2-4 ONS 15310-CL and ONS 15310-MA NA Conditions List (continued)

FRCDSWTOTHIRD (NE-SREF)	SD-P (STSTRM)	WKSWPR (EQPT)
FRNGSYNC (NE-SREF)	SD-V (VT-MON)	WKSWPR (OCN)
FSTSYNC (NE-SREF)	SD-V (VT-TERM)	WKSWPR (STSMON)
FULLPASSTHR-BI (OCN)	SF (DS1)	WKSWPR (VT-MON)
HLDOVRSYNC (NE-SREF)	SF (DS3)	WTR (EQPT)
IDLE (DS1)	SF-L (EC1)	WTR (OCN)
INC-ISD (DS3)	SF-L (OCN)	WTR (STSMON)
INHSWPR (EQPT)	SF-P (STSMON)	WTR (VT-MON)

2.1.5 Not Reported (NR) Conditions

Table 2-2 alphabetically lists ONS 15310-CL and ONS 15310-MA Major (MJ) alarms.

Table 2-5 ONS 15310-CL and ONS 15310-MA Major Alarm List

AIS (BITS)	AUTOSW-AIS (STSMON)	RFI-L (OCN)
AIS (DS1)	AUTOSW-AIS (VT-MON)	RFI-P (STSMON)
AIS (DS3)	BERT-ENBL (DS1, DS3)	RFI-P (STSTRM)
AIS (FUDC)	BERT-SYNC-FAIL (DS1, DS3)	RFI-V (VT-MON)
AIS-L (EC1)	ERFI-P-CONN (STSMON)	RFI-V (VT-TERM)
AIS-L (OCN)	ERFI-P-CONN (STSTRM)	ROLL-PEND (STSTRM)
AIS-P (STSMON)	ERFI-P-PAYLD (STSMON)	TX-AIS (DS1)
AIS-P (STSTRM)	ERFI-P-PAYLD (STSTRM)	TX-AIS (DS3)
AIS-V (VT-MON)	NON-CISCO-PPM (PPM)	TX-LOF (DS1)
AIS-V (VT-TERM)	RFI-L (EC1)	UNQUAL-PPM (PPM)

2.2 Alarms and Conditions Indexed By Alphabetical Entry

Table 2-6 alphabetically lists all ONS 15310-CL and ONS 15310-MA alarms and conditions.

Table 2-6 ONS 15310-CL and ONS 15310-MA Alarm and Condition Alphabetical List

AIS (BITS)	GFP-CSF (CE100T)	ROLL (STSMON)
AIS (DS1)	GFP-CSF (CEMR)	ROLL (STSTRM)
AIS (DS3)	GFP-CSF (ML100T)	ROLL (VT-MON)
AIS (FUDC)	GFP-LFD (CE100T)	ROLL (VT-TERM)
AIS-L (EC1)	GFP-LFD (CEMR)	ROLL-PEND (STSMON)
AIS-L (OCN)	GFP-LFD (ML100T)	ROLL-PEND (STSTRM)
AIS-P (STSMON)	GFP-UP-MISMATCH (CE100T)	ROLL-PEND (VT-MON)

Table 2-6 ONS 15310-CL and ONS 15310-MA Alarm and Condition Alphabetical List (continued)

AIS-P (STSTRM)	GFP-UP-MISMATCH (CEMR)	ROLL-PEND (VT-TERM)
AIS-V (VT-MON)	GFP-UP-MISMATCH (ML100T)	RPR-PASSTHR (RPRIF)
AIS-V (VT-TERM)	HELLO (OCN)	RPRW (ML100T)
ALS (OCN)	HI-LASERBIAS (OCN)	RUNCFG-SAVENEED (EQPT)
APC-END (NE)	HI-LASERBIAS (PPM)	SD (DS1)
APSB (OCN)	HI-LASERTEMP (OCN)	SD (DS3)
APSCDFLTK (OCN)	HI-LASERTEMP (PPM)	SD-L (EC1)
APSCINCON (OCN)	HI-RXPOWER (OCN)	SD-L (OCN)
APSCM (OCN)	HITEMP (EQPT)	SD-P (STSMON)
APSCNMIS (OCN)	HITEMP (NE)	SD-P (STSTRM)
APSIMP (OCN)	HI-TXPOWER (OCN)	SD-V (VT-MON)
APS-INV-PRIM (OCN)	HI-TXPOWER (PPM)	SD-V (VT-TERM)
APSMM (OCN)	HLDOVRSYNC (NE-SREF)	SF (DS1)
APS-PRIM-FAC (OCN)	IDLE (DS1)	SF (DS3)
APS-PRIM-SEC-MISM (OCN)	I-HITEMP (NE)	SF-L (EC1)
AS-CMD (BPLANE)	IMPROPRMVL (EQPT)	SF-L (OCN)
AS-CMD (CE100T)	IMPROPRMVL (PPM)	SF-P (STSMON)
AS-CMD (CEMR)	INC-ISD (DS3)	SF-P (STSTRM)
AS-CMD (DS1)	INHSWPR (EQPT)	SFTWDOWN (EQPT)
AS-CMD (DS3)	INHSWWKG (EQPT)	SF-V (VT-MON)
AS-CMD (EC1)	INTRUSION-PSWD (NE)	SF-V (VT-TERM)
AS-CMD (EQPT)	INVMACADR (BPLANE)	SHELF-COMM-FAIL (SHELF)
AS-CMD (ML100T)	IOSCFGCOPY (EQPT)	SNTP-HOST (NE)
AS-CMD (NE)	ISIS-ADJ-FAIL (OCN)	SQM (STSTRM)
AS-CMD (OCN)	KB-PASSTHR (OCN)	SQM (VT-TERM)
AS-CMD (PPM)	LASEREOL (OCN)	SSM-DUS (BITS)
AS-CMD (PWR)	LCAS-CRC (STSTRM)	SSM-DUS (DS1)
AS-CMD (SHELF)	LCAS-CRC (VT-TERM)	SSM-DUS (OCN)
AS-MT (CE100T)	LCAS-RX-DNU (STSTRM)	SSM-FAIL (BITS)
AS-MT (CEMR)	LCAS-RX-DNU (VT-TERM)	SSM-FAIL (DS1)
AS-MT (DS1)	LCAS-RX-FAIL (STSTRM)	SSM-FAIL (OCN)
AS-MT (DS3)	LCAS-RX-FAIL (VT-TERM)	SSM-LNC (BITS)
AS-MT (EC1)	LCAS-RX-GRP-ERR (STSTRM)	SSM-LNC (NE-SREF)
AS-MT (EQPT)	LCAS-RX-GRP-ERR (VT-TERM)	SSM-LNC (OCN)
AS-MT (ML100T)	LCAS-TX-ADD (STSTRM)	SSM-OFF (BITS)
AS-MT (OCN)	LCAS-TX-ADD (VT-TERM)	SSM-OFF (DS1)
AS-MT (PPM)	LCAS-TX-DNU (STSTRM)	SSM-OFF (OCN)

Table 2-6 ONS 15310-CL and ONS 15310-MA Alarm and Condition Alphabetical List (continued)

AS-MT (SHELF)	LCAS-TX-DNU (VT-TERM)	SSM-PRC (BITS)
AS-MT-OOG (STSTRM)	LINK-KEEPALIVE (ML100T)	SSM-PRC (NE-SREF)
AS-MT-OOG (VT-TERM)	LKOUTPR-S (OCN)	SSM-PRC (OCN)
AUD-LOG-LOSS (NE)	LOA (VCG)	SSM-PRS (BITS)
AUD-LOG-LOW (NE)	LOCKOUT-REQ (OCN)	SSM-PRS (DS1)
AUTOLSROFF (OCN)	LOCKOUT-REQ (STSMON)	SSM-PRS (NE-SREF)
AUTORESET (EQPT)	LOCKOUT-REQ (VT-MON)	SSM-PRS (OCN)
AUTOSW-AIS (STSMON)	LOF (BITS)	SSM-RES (BITS)
AUTOSW-AIS (VT-MON)	LOF (DS1)	SSM-RES (DS1)
AUTOSW-LOP (STSMON)	LOF (DS3)	SSM-RES (NE-SREF)
AUTOSW-LOP (VT-MON)	LOF (EC1)	SSM-RES (OCN)
AUTOSW-PDI (STSMON)	LOF (OCN)	SSM-SDH-TN (BITS)
AUTOSW-PDI (VT-MON)	LOF (STSTRM)	SSM-SDH-TN (NE-SREF)
AUTOSW-SDBER (STSMON)	LO-LASERBIAS (OCN)	SSM-SDH-TN (OCN)
AUTOSW-SDBER (VT-MON)	LO-LASERBIAS (PPM)	SSM-SETS (BITS)
AUTOSW-SFBER (STSMON)	LO-LASERTEMP (OCN)	SSM-SETS (NE-SREF)
AUTOSW-SFBER (VT-MON)	LO-LASERTEMP (PPM)	SSM-SETS (OCN)
AUTOSW-UNEQ (STSMON)	LOM (STSMON)	SSM-SMC (BITS)
AUTOSW-UNEQ (VT-MON)	LOM (STSTRM)	SSM-SMC (DS1)
BAT-FAIL (PWR)	LOM (VT-TERM)	SSM-SMC (NE-SREF)
BERT-ENBL (DS1, DS3)	LOP-P (STSMON)	SSM-SMC (OCN)
BERT-SYNC-FAIL (DS1, DS3)	LOP-P (STSTRM)	SSM-ST2 (BITS)
BKUPMEMP (EQPT)	LOP-V (VT-MON)	SSM-ST2 (DS1)
BLSROSYNC (OCN)	LOP-V (VT-TERM)	SSM-ST2 (NE-SREF)
CARLOSS (CE100T)	LO-RXPOWER (OCN)	SSM-ST2 (OCN)
CARLOSS (CEMR)	LOS (BITS)	SSM-ST3 (BITS)
CARLOSS (EQPT)	LOS (DS1)	SSM-ST3 (DS1)
CARLOSS (ML100T)	LOS (DS3)	SSM-ST3 (NE-SREF)
CLDRESTART (EQPT)	LOS (EC1)	SSM-ST3 (OCN)
COMIOXC (EQPT)	LOS (FUDC)	SSM-ST3E (BITS)
CONTBUS-CLK-A (EQPT)	LOS (OCN)	SSM-ST3E (DS1)
CONTBUS-CLK-B (EQPT)	LO-TXPOWER (OCN)	SSM-ST3E (NE-SREF)
CONTBUS-DISABLED (EQPT)	LO-TXPOWER (PPM)	SSM-ST3E (OCN)
CONTBUS-IO-A (EQPT)	LPBKCRS (STSMON)	SSM-ST4 (BITS)
CONTBUS-IO-B (EQPT)	LPBKCRS (STSTRM)	SSM-ST4 (DS1)
CTNEQPT-PBPROT (EQPT)	LPBKDS1FE-CMD (DS1)	SSM-ST4 (NE-SREF)
CTNEQPT-PBWORK (EQPT)	LPBKDS3FEAC (DS3)	SSM-ST4 (OCN)

Table 2-6 ONS 15310-CL and ONS 15310-MA Alarm and Condition Alphabetical List (continued)

DATA-CRC (CE100T)	LPBKDS3FEAC-CMD (DS3)	SSM-STU (BITS)
DATA-CRC (ML100T)	LPBKFACILITY (CE100T)	SSM-STU (DS1)
DATAFLT (NE)	LPBKFACILITY (CEMR)	SSM-STU (NE-SREF)
DS3-MISM (DS3)	LPBKFACILITY (DS1)	SSM-STU (OCN)
DUP-IPADDR (NE)	LPBKFACILITY (DS3)	SSM-TNC (BITS)
DUP-NODENAME (NE)	LPBKFACILITY (EC1)	SSM-TNC (NE-SREF)
DUP-SHELF-ID (SHELF)	LPBKFACILITY (OCN)	SSM-TNC (OCN)
EHIBATVG (PWR)	LPBKTERMINAL (CE100T)	SW-MISMATCH (EQPT)
ELWBATVG (PWR)	LPBKTERMINAL (CEMR)	SWMTXMOD-PROT (EQPT)
ENCAP-MISMATCH-P (STSTRM)	LPBKTERMINAL (DS1)	SWMTXMOD-WORK (EQPT)
EOC (OCN)	LPBKTERMINAL (DS3)	SWTOPRI (EXT-SREF)
EOC-L (OCN)	LPBKTERMINAL (EC1)	SWTOPRI (NE-SREF)
EQPT (EQPT)	LPBKTERMINAL (OCN)	SWTOSEC (EXT-SREF)
EQPT (PPM)	MAN-REQ (STSMON)	SWTOSEC (NE-SREF)
EQPT-MISS (FAN)	MAN-REQ (VT-MON)	SWTOTHIRD (EXT-SREF)
ERFI-P-CONN (STSMON)	MANRESET (EQPT)	SWTOTHIRD (NE-SREF)
ERFI-P-CONN (STSTRM)	MANSWTOINT (NE-SREF)	SYNC-FREQ (BITS)
ERFI-P-PAYLD (STSMON)	MANSWTOPRI (EXT-SREF)	SYNC-FREQ (DS1)
ERFI-P-PAYLD (STSTRM)	MANSWTOPRI (NE-SREF)	SYNC-FREQ (OCN)
ERROR-CONFIG (EQPT)	MANSWTOSEC (EXT-SREF)	SYNCPRI (EXT-SREF)
ETH-LINKLOSS (NE)	MANSWTOSEC (NE-SREF)	SYNCPRI (NE-SREF)
EXCCOL (EQPT)	MANSWTOTHIRD (EXT-SREF)	SYNCSEC (EXT-SREF)
EXT (ENVALRM)	MANSWTOTHIRD (NE-SREF)	SYNCSEC (NE-SREF)
FAILTOSW (OCN)	MANUAL-REQ-SPAN (OCN)	SYNCTHIRD (EXT-SREF)
FAILTOSW-PATH (STSMON)	MATECLK (EQPT)	SYNCTHIRD (NE-SREF)
FAILTOSW-PATH (VT-MON)	MEA (EQPT)	SYSBOOT (NE)
FAN (FAN)	MEA (FAN)	TIM (OCN)
FANDEGRADE (FAN)	MEA (PPM)	TIM-P (STSMON)
FE-AIS (DS3)	MEA (SHELF)	TIM-P (STSTRM)
FE-DS1-MULTLOS (DS3)	MEM-GONE (EQPT)	TIM-S (EC1)
FE-DS1-NSA (DS3)	MEM-LOW (EQPT)	TIM-S (OCN)
FE-DS1-SA (DS3)	MFGMEM (BPLANE)	TIM-V (VT-MON)
FE-DS1-SNGLLOS (DS3)	MFGMEM (FAN)	TIM-V (VT-TERM)
FE-DS3-NSA (DS3)	MFGMEM (PPM)	TPTFAIL (CE100T)
FE-DS3-SA (DS3)	NO-CONFIG (EQPT)	TPTFAIL (CEMR)
FE-EQPT-NSA (DS3)	NON-CISCO-PPM (PPM)	TPTFAIL (ML100T)
FE-FRCDWKSWBK-SPAN (OCN)	OOU-TPT (STSTRM)	TX-AIS (DS1)

Table 2-6 ONS 15310-CL and ONS 15310-MA Alarm and Condition Alphabetical List (continued)

FE-FRCDWKSWPR-SPAN (OCN)	OOU-TPT (VT-TERM)	TX-AIS (DS3)
FE-IDLE (DS3)	OPEN-SLOT (EQPT)	TX-IDLE (DS1)
FE-LOCKOUTOFPR-SPAN (OCN)	PDI-P (STSMON)	TX-LOF (DS1)
FE-LOF (DS3)	PDI-P (STSTRM)	TX-RAI (DS1)
FE-LOS (DS3)	PLM-P (STSMON)	TX-RAI (DS3)
FE-MANWKSWBK-SPAN (OCN)	PLM-P (STSTRM)	UNEQ-P (STSMON)
FE-MANWKSWPR-SPAN (OCN)	PLM-V (VT-MON)	UNEQ-P (STSTRM)
FEPRLF (OCN)	PLM-V (VT-TERM)	UNEQ-V (VT-MON)
FORCED-REQ (STSMON)	PORT-MISMATCH (CEMR)	UNEQ-V (VT-TERM)
FORCED-REQ (VT-MON)	PRC-DUPID (OCN)	UNQUAL-PPM (PPM)
FORCED-REQ-SPAN (OCN)	PROTNA (EQPT)	VCG-DEG (VCG)
FP-LINK-LOSS (EQPT)	PROV-MISMATCH (PPM)	VCG-DOWN (VCG)
FRCDSWTOINT (NE-SREF)	PWR-FAIL-A (EQPT)	WKSWPR (EQPT)
FRCDSWTOPRI (EXT-SREF)	PWR-FAIL-B (EQPT)	WKSWPR (OCN)
FRCDSWTOPRI (NE-SREF)	RAI (DS1)	WKSWPR (STSMON)
FRCDSWTOSEC (EXT-SREF)	RAI (DS3)	WKSWPR (VT-MON)
FRCDSWTOSEC (NE-SREF)	RFI-L (EC1)	WTR (EQPT)
FRCDSWTOTHIRD (EXT-SREF)	RFI-L (OCN)	WTR (OCN)
FRCDSWTOTHIRD (NE-SREF)	RFI-P (STSMON)	WTR (STSMON)
FRNGSYNC (NE-SREF)	RFI-P (STSTRM)	WTR (VT-MON)
FSTSYNC (NE-SREF)	RFI-V (VT-MON)	—
FULLPASSTHR-BI (OCN)	RFI-V (VT-TERM)	—

2.3 Alarm Logical Objects

The CTC alarm profile list organizes all alarms and conditions according to the logical objects they are raised against. These logical objects represent physical objects such as cards, logical objects such as circuits, or transport and signal monitoring entities such as the SONET overhead bits. One alarm can appear in multiple entries. It can be raised against multiple objects. For example, the loss of signal (LOS) alarm can be raised against the optical signal (OC-N) or the optical transport layer overhead (OTN) as well as other objects. Therefore, both OCN: LOS and OTN: LOS appear in the list (as well as the other objects).

Alarm profile list objects are defined in Table 2-7.

Note Alarm logical object names can appear as abbreviated versions of standard terms used in the system and the documentation. For example, the “OCN” logical object refers to the OC-N signal. Logical object names or industry-standard terms are used within the entries as appropriate.

Table 2-7 Alarm Logical Object Type Definitions

Type	Definition
BITS	Building integrated timing supply (BITS) incoming references (BITS-1, BITS-2).
BPLANE	The backplane.
CE100T	The CE-100T-8 Ethernet card.
CEMR	The CE-MR-6 Ethernet card.
DS1	A DS-1 port on the 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card.
DS3	A DS-3 port on the 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card.
EC1	A EC-1 port on the 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card.
ENVALRM	An environmental alarm port.
EQPT	A card, its physical objects, and logical objects as they are located in any of the noncommon card slots. The EQPT object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, synchronous transport signal (STS), and virtual tributary (VT).
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
FAN	Fan located in the ONS 15310-CL or ONS 15310-MA shelf.
FUDC	SONET F1 byte user data channel for an ONS 15310-CL or ONS 15310-MA ML-100T-8 Ethernet card.
ML100T	The ML-100T-8 Ethernet card.
NE	The entire network element.
NE-SREF	The timing status of the NE.
OCN	An OC-3 port or OC-12 port on the 15310-CL-CTX or CTX2500 card.
PPM	Pluggable port module (PPM, also called SFP).
RPRIF	Interface for Resilient Packet Ring technology as defined in IEEE 802.17b. Also called RPR-IEEE.
PWR	The node power supply.
SHELF	The ONS 15310-CL or ONS 15310-MA shelf.
STSMON	STS alarm detection at the monitor point (upstream from the cross-connect). **Note** The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of STSMON, if available, should be changed to the same severity as the customized severity for a specific STS alarm.
STSTRM	STS alarm detection at termination (downstream from the cross-connect). **Note** The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of STSTRM, if available, should be changed to the same severity as the customized severity for a specific STS alarm.

Table 2-7 Alarm Logical Object Type Definitions (continued)

Type	Definition
VCG	Virtual concatenation group.
VT-MON	VT1 alarm detection at the monitor point (upstream from the cross-connect). **Note** The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of VT-MON, if available, should be changed to the same severity as the customized severity for a specific VT alarm.
VT-TERM	VT1 alarm detection at termination (downstream from the cross-connect). **Note** The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of VT-TERM, if available, should be changed to the same severity as the customized severity for a specific VT alarm.

2.4 Alarm List by Logical Object Type

Table 2-8 lists all ONS 15310-CL and ONS 15310-MA Release 9.0 alarms and logical objects as they are given in the system alarm profile. The list entries are organized by logical object name and then by alarm or condition name. Where appropriate, the alarm entries also contain troubleshooting procedures.

Note The list is given here exactly as it is shown in CTC, and in some cases does not follow alphabetical order.

Table 2-8 ONS 15310-CL and ONS 15310-MA Alarm List by Logical Object as Shown in Alarm Profile

BITS: AIS (NR)	EQPT: MEM-GONE (MJ)	OCN: SSM-PRC (NA)
BITS: LOF (MN)	EQPT: MEM-LOW (MN)	OCN: SSM-PRS (NA)
BITS: LOS (MN)	EQPT: NO-CONFIG (NA)	OCN: SSM-RES (NA)
BITS: SSM-DUS (NA)	EQPT: OPEN-SLOT (NA)	OCN: SSM-SDH-TN (NA)
BITS: SSM-FAIL (MN)	EQPT: PROTNA (MN)	OCN: SSM-SETS (NA)
BITS: SSM-LNC (NA)	EQPT: PWR-FAIL-A (MN)	OCN: SSM-SMC (NA)
BITS: SSM-OFF (NA)	EQPT: PWR-FAIL-B (MN)	OCN: SSM-ST2 (NA)
BITS: SSM-PRC (NA)	EQPT: RUNCFG-SAVENEED (NA)	OCN: SSM-ST3 (NA)
BITS: SSM-PRS (NA)	EQPT: SFTWDOWN (MN)	OCN: SSM-ST3E (NA)
BITS: SSM-RES (NA)	EQPT: SW-MISMATCH (NA)	OCN: SSM-ST4 (NA)
BITS: SSM-SDH-TN (NA)	EQPT: SWMTXMOD-PROT (CR)	OCN: SSM-STU (NA)
BITS: SSM-SETS (NA)	EQPT: SWMTXMOD-WORK (CR)	OCN: SSM-TNC (NA)
BITS: SSM-SMC (NA)	EQPT: WKSWPR (NA)	OCN: SYNC-FREQ (NA)
BITS: SSM-ST2 (NA)	EQPT: WTR (NA)	OCN: TIM (CR)
BITS: SSM-ST3 (NA)	EXT-SREF: FRCDSWTOPRI (NA)	OCN: TIM-S (CR)

Table 2-8 ONS 15310-CL and ONS 15310-MA Alarm List by Logical Object as Shown in Alarm Profile (continued)

BITS: SSM-ST3E (NA)	EXT-SREF: FRCDSWTOSEC (NA)	OCN: WKSWPR (NA)
BITS: SSM-ST4 (NA)	EXT-SREF: FRCDSWTOTHIRD (NA)	OCN: WTR (NA)
BITS: SSM-STU (NA)	EXT-SREF: MANSWTOPRI (NA)	PPM: AS-CMD (NA)
BITS: SSM-TNC (NA)	EXT-SREF: MANSWTOSEC (NA)	PPM: AS-MT (NA)
BITS: SYNC-FREQ (NA)	EXT-SREF: MANSWTOTHIRD (NA)	PPM: EQPT (CR)
BPLANE: AS-CMD (NA)	EXT-SREF: SWTOPRI (NA)	PPM: HI-LASERBIAS (MN)
BPLANE: INVMACADR (MJ)	EXT-SREF: SWTOSEC (NA)	PPM: HI-LASERTEMP (MN)
BPLANE: MFGMEM (CR)	EXT-SREF: SWTOTHIRD (NA)	PPM: HI-TXPOWER (MN)
CE100T: AS-CMD (NA)	EXT-SREF: SYNCPRI (MN)	PPM: IMPROPRMVL (CR)
CE100T: AS-MT (NA)	EXT-SREF: SYNCSEC (MN)	PPM: LO-LASERBIAS (MN)
CE100T: CARLOSS (MJ)	EXT-SREF: SYNCTHIRD (MN)	PPM: LO-LASERTEMP (MN)
CE100T: DATA-CRC (MJ)	FAN: EQPT-MISS (CR)	PPM: LO-TXPOWER (MN)
CE100T: GFP-CSF (MJ)	FAN: FAN (CR)	PPM: MEA (CR)
CE100T: GFP-LFD (MJ)	FAN: FANDEGRADE (MJ)	PPM: MFGMEM (CR)
CE100T: GFP-UP-MISMATCH (MJ)	FAN: MEA (CR)	PPM: NON-CISCO-PPM (NR)
CE100T: LPBKFACILITY (NA)	FAN: MFGMEM (CR)	PPM: PROV-MISMATCH (MN)
CE100T: LPBKTERMINAL (NA)	FUDC: AIS (NR)	PPM: UNQUAL-PPM (NR)
CE100T: TPTFAIL (MJ)	FUDC: LOS (MN)	PWR: AS-CMD (NA)
CEMR: AS-CMD (NA)	ML100T: AS-CMD (NA)	PWR: BAT-FAIL (MJ)
CEMR: AS-MT (NA)	ML100T: AS-MT (NA)	PWR: EHIBATVG (MJ)
CEMR: CARLOSS (MJ)	ML100T: CARLOSS (MJ)	PWR: ELWBATVG (MJ)
CEMR: GFP-CSF (MJ)	ML100T: DATA-CRC (MJ)	RPRIF: RPR-PASSTHR (NA)
CEMR: GFP-LFD (MJ)	ML100T: GFP-CSF (MJ)	SHELF: AS-CMD (NA)
CEMR: GFP-UP-MISMATCH (MJ)	ML100T: GFP-LFD (MJ)	SHELF: AS-MT (NA)
CEMR: LPBKFACILITY (NA)	ML100T: GFP-UP-MISMATCH (MJ)	SHELF: DUP-SHELF-ID (MJ)
CEMR: LPBKTERMINAL (NA)	ML100T: LINK-KEEPALIVE (CR)	SHELF: MEA (MJ)
CEMR: PORT-MISMATCH (MJ)	ML100T: RPRW (NA)	SHELF: SHELF-COMM-FAIL (MJ)
CEMR: TPTFAIL (MJ)	ML100T: TPTFAIL (MJ)	STSMON: AIS-P (NR)
DS1: AIS (NR)	NE: APC-END (NA)	STSMON: AUTOSW-AIS (NR)
DS1: AS-CMD (NA)	NE: AS-CMD (NA)	STSMON: AUTOSW-LOP (NA)
DS1: AS-MT (NA)	NE: AUD-LOG-LOSS (NA)	STSMON: AUTOSW-PDI (NA)
DS1: BERT-ENBL (NR)	NE: AUD-LOG-LOW (NA)	STSMON: AUTOSW-SDBER (NA)
DS1: BERT-SYNC-FAIL (NR)	NE: DATAFLT (MN)	STSMON: AUTOSW-SFBER (NA)
DS1: IDLE (NA)	NE: DUP-IPADDR (MN)	STSMON: AUTOSW-UNEQ (NA)
DS1: LOF (MJ)	NE: DUP-NODENAME (MN)	STSMON: ERFI-P-CONN (NR)
DS1: LOS (MJ)	NE: ETH-LINKLOSS (NA)	STSMON: ERFI-P-PAYLD (NR)
DS1: LPBKDS1FE-CMD (NA)	NE: HITEMP (CR)	STSMON: FAILTOSW-PATH (NA)

Table 2-8 ONS 15310-CL and ONS 15310-MA Alarm List by Logical Object as Shown in Alarm Profile (continued)

DS1: LPBKFACILITY (NA)	NE: I-HITEMP (CR)	STSMON: FORCED-REQ (NA)
DS1: LPBKTERMINAL (NA)	NE: INTRUSION-PSWD (NA)	STSMON: LOCKOUT-REQ (NA)
DS1: RAI (NA)	NE: SNTP-HOST (MN)	STSMON: LOM (CR)
DS1: SD (NA)	NE: SYSBOOT (MJ)	STSMON: LOP-P (CR)
DS1: SF (NA)	NE-SREF: FRCDSWTOINT (NA)	STSMON: LPBKCRS (NA)
DS1: SSM-DUS (NA)	NE-SREF: FRCDSWTOPRI (NA)	STSMON: MAN-REQ (NA)
DS1: SSM-FAIL (MN)	NE-SREF: FRCDSWTOSEC (NA)	STSMON: PDI-P (NA)
DS1: SSM-OFF (NA)	NE-SREF: FRCDSWTOTHIRD (NA)	STSMON: PLM-P (CR)
DS1: SSM-PRS (NA)	NE-SREF: FRNGSYNC (NA)	STSMON: RFI-P (NR)
DS1: SSM-RES (NA)	NE-SREF: FSTSYNC (NA)	STSMON: ROLL (NA)
DS1: SSM-SMC (NA)	NE-SREF: HLDOVRSYNC (NA)	STSMON: ROLL-PEND (NA)
DS1: SSM-ST2 (NA)	NE-SREF: MANSWTOINT (NA)	STSMON: SD-P (NA)
DS1: SSM-ST3 (NA)	NE-SREF: MANSWTOPRI (NA)	STSMON: SF-P (NA)
DS1: SSM-ST3E (NA)	NE-SREF: MANSWTOSEC (NA)	STSMON: TIM-P (MN)
DS1: SSM-ST4 (NA)	NE-SREF: MANSWTOTHIRD (NA)	STSMON: UNEQ-P (CR)
DS1: SSM-STU (NA)	NE-SREF: SSM-LNC (NA)	STSMON: WKSWPR (NA)
DS1: SYNC-FREQ (NA)	NE-SREF: SSM-PRC (NA)	STSMON: WTR (NA)
DS1: TX-AIS (NR)	NE-SREF: SSM-PRS (NA)	STSTRM: AIS-P (NR)
DS1: TX-IDLE (NA)	NE-SREF: SSM-RES (NA)	STSTRM: AS-MT-OOG (NA)
DS1: TX-LOF (NR)	NE-SREF: SSM-SDH-TN (NA)	STSTRM: ENCAP-MISMATCH-P (CR)
DS1: TX-RAI (NA)	NE-SREF: SSM-SETS (NA)	STSTRM: ERFI-P-CONN (NR)
DS3: AIS (NR)	NE-SREF: SSM-SMC (NA)	STSTRM: ERFI-P-PAYLD (NR)
DS3: AS-CMD (NA)	NE-SREF: SSM-ST2 (NA)	STSTRM: LCAS-CRC (NA)
DS3: AS-MT (NA)	NE-SREF: SSM-ST3 (NA)	STSTRM: LCAS-RX-DNU (NA)
DS3: BERT-ENBL (NR)	NE-SREF: SSM-ST3E (NA)	STSTRM: LCAS-RX-FAIL (NA)
DS3: BERT-SYNC-FAIL (NR)	NE-SREF: SSM-ST4 (NA)	STSTRM: LCAS-RX-GRP-ERR (NA)
DS3: DS3-MISM (NA)	NE-SREF: SSM-STU (NA)	STSTRM: LCAS-TX-ADD (NA)
DS3: FE-AIS (NA)	NE-SREF: SSM-TNC (NA)	STSTRM: LCAS-TX-DNU (NA)
DS3: FE-DS1-MULTLOS (NA)	NE-SREF: SWTOPRI (NA)	STSTRM: LOF (CR)
DS3: FE-DS1-NSA (NA)	NE-SREF: SWTOSEC (NA)	STSTRM: LOM (CR)
DS3: FE-DS1-SA (NA)	NE-SREF: SWTOTHIRD (NA)	STSTRM: LOP-P (CR)
DS3: FE-DS1-SNGLLOS (NA)	NE-SREF: SYNCPRI (MJ)	STSTRM: LPBKCRS (NA)
DS3: FE-DS3-NSA (NA)	NE-SREF: SYNCSEC (MN)	STSTRM: OOU-TPT (NA)
DS3: FE-DS3-SA (NA)	NE-SREF: SYNCTHIRD (MN)	STSTRM: PDI-P (NA)
DS3: FE-EQPT-NSA (NA)	OCN: AIS-L (NR)	STSTRM: PLM-P (CR)
DS3: FE-IDLE (NA)	OCN: ALS (NA)	STSTRM: RFI-P (NR)
DS3: FE-LOF (NA)	OCN: APSB (MN)	STSTRM: ROLL (NA)

Table 2-8 ONS 15310-CL and ONS 15310-MA Alarm List by Logical Object as Shown in Alarm Profile (continued)

DS3: FE-LOS (NA)	OCN: APSCDFLTK (MN)	STSTRM: ROLL-PEND (NR)
DS3: INC-ISD (NA)	OCN: APSCINCON (MN)	STSTRM: SD-P (NA)
DS3: LOF (CR)	OCN: APSCM (MN)	STSTRM: SF-P (NA)
DS3: LOS (CR)	OCN: APSCNMIS (MJ)	STSTRM: SQM (CR)
DS3: LPBKDS3FEAC (NA)	OCN: APSIMP (MN)	STSTRM: TIM-P (CR)
DS3: LPBKDS3FEAC-CMD (NA)	OCN: APS-INV-PRIM (MN)	STSTRM: UNEQ-P (CR)
DS3: LPBKFACILITY (NA)	OCN: APSMM (MN)	VCG: LOA (CR)
DS3: LPBKTERMINAL (NA)	OCN: APS-PRIM-FAC (NA)	VCG: VCG-DEG (NA)
DS3: RAI (NA)	OCN: APS-PRIM-SEC-MISM (MN)	VCG: VCG-DOWN (NA)
DS3: SD (NA)	OCN: AS-CMD (NA)	VT-MON: AIS-V (NR)
DS3: SF (NA)	OCN: AS-MT (NA)	VT-MON: AUTOSW-AIS (NR)
DS3: TX-AIS (NR)	OCN: AUTOLSROFF (CR)	VT-MON: AUTOSW-LOP (NA)
DS3: TX-RAI (NA)	OCN: BLSROSYNC (MJ)	VT-MON: AUTOSW-PDI (NA)
EC1: AIS-L (NR)	OCN: EOC (MN)	VT-MON: AUTOSW-SDBER (NA)
EC1: AS-CMD (NA)	OCN: EOC-L (MN)	VT-MON: AUTOSW-SFBER (NA)
EC1: AS-MT (NA)	OCN: FAILTOSW (NA)	VT-MON: AUTOSW-UNEQ (NA)
EC1: LOF (CR)	OCN: FE-FRCDWKSWBK-SPAN (NA)	VT-MON: FAILTOSW-PATH (NA)
EC1: LOS (CR)	OCN: FE-FRCDWKSWPR-SPAN (NA)	VT-MON: FORCED-REQ (NA)
EC1: LPBKFACILITY (NA)	OCN: FE-LOCKOUTOFPR-SPAN (NA)	VT-MON: LOCKOUT-REQ (NA)
EC1: LPBKTERMINAL (NA)	OCN: FE-MANWKSWBK-SPAN (NA)	VT-MON: LOP-V (MJ)
EC1: RFI-L (NR)	OCN: FE-MANWKSWPR-SPAN (NA)	VT-MON: MAN-REQ (NA)
EC1: SD-L (NA)	OCN: FEPRLF (MN)	VT-MON: PLM-V (MJ)
EC1: SF-L (NA)	OCN: FORCED-REQ-SPAN (NA)	VT-MON: RFI-V (NR)
EC1: TIM-S (CR)	OCN: FULLPASSTHR-BI (NA)	VT-MON: ROLL (NA)
ENVALRM: EXT (MN)	OCN: HELLO (MN)	VT-MON: ROLL-PEND (NA)
EQPT: AS-CMD (NA)	OCN: HI-LASERBIAS (MN)	VT-MON: SD-V (NA)
EQPT: AS-MT (NA)	OCN: HI-LASERTEMP (MN)	VT-MON: SF-V (NA)
EQPT: AUTORESET (MN)	OCN: HI-RXPOWER (MN)	VT-MON: TIM-V (MJ)
EQPT: BKUPMEMP (CR)	OCN: HI-TXPOWER (MN)	VT-MON: UNEQ-V (MJ)
EQPT: CARLOSS (MJ)	OCN: ISIS-ADJ-FAIL (MN)	VT-MON: WKSWPR (NA)
EQPT: CLDRESTART (NA)	OCN: KB-PASSTHR (NA)	VT-MON: WTR (NA)
EQPT: COMIOXC (CR)	OCN: LASEREOL (MN)	VT-TERM: AIS-V (NR)
EQPT: CONTBUS-CLK-A (MN)	OCN: LKOUTPR-S (NA)	VT-TERM: AS-MT-OOG (NA)
EQPT: CONTBUS-CLK-B (MN)	OCN: LOCKOUT-REQ (NA)	VT-TERM: LCAS-CRC (NA)
EQPT: CONTBUS-DISABLED (CR)	OCN: LOF (CR)	VT-TERM: LCAS-RX-DNU (NA)
EQPT: CONTBUS-IO-A (MN)	OCN: LO-LASERBIAS (MN)	VT-TERM: LCAS-RX-FAIL (NA)
EQPT: CONTBUS-IO-B (MN)	OCN: LO-LASERTEMP (MN)	VT-TERM: LCAS-RX-GRP-ERR (NA)

Table 2-8 ONS 15310-CL and ONS 15310-MA Alarm List by Logical Object as Shown in Alarm Profile (continued)

EQPT: CTNEQPT-PBPROT (CR)	OCN: LO-RXPOWER (MN)	VT-TERM: LCAS-TX-ADD (NA)
EQPT: CTNEQPT-PBWORK (CR)	OCN: LOS (CR)	VT-TERM: LCAS-TX-DNU (NA)
EQPT: EQPT (CR)	OCN: LO-TXPOWER (MN)	VT-TERM: LOM (MJ)
EQPT: ERROR-CONFIG (MN)	OCN: LPBKFACILITY (NA)	VT-TERM: LOP-V (MJ)
EQPT: EXCCOL (MN)	OCN: LPBKTERMINAL (NA)	VT-TERM: OOU-TPT (NA)
EQPT: FP-LINK-LOSS (MN)	OCN: MANUAL-REQ-SPAN (NA)	VT-TERM: PLM-V (MJ)
EQPT: HITEMP (MN)	OCN: PRC-DUPID (MJ)	VT-TERM: RFI-V (NR)
EQPT: IMPROPRMVL (CR)	OCN: RFI-L (NR)	VT-TERM: ROLL (NA)
EQPT: INHSWPR (NA)	OCN: SD-L (NA)	VT-TERM: ROLL-PEND (NA)
EQPT: INHSWWKG (NA)	OCN: SF-L (NA)	VT-TERM: SD-V (NA)
EQPT: IOSCFGCOPY (NA)	OCN: SSM-DUS (NA)	VT-TERM: SF-V (NA)
EQPT: MANRESET (NA)	OCN: SSM-FAIL (MN)	VT-TERM: SQM (MJ)
EQPT: MATECLK (MN)	OCN: SSM-LNC (NA)	VT-TERM: TIM-V (MJ)
EQPT: MEA (CR)	OCN: SSM-OFF (NA)	VT-TERM: UNEQ-V (MJ)

2.5 Trouble Notifications

The ONS 15310-CL and ONS 15310-MA systems report trouble by utilizing standard alarm and condition characteristics, standard severities following the rules in Telcordia GR-253-CORE, and graphical user interface (GUI) state indicators. These notifications are described in the following sections.

The ONS 15310-CL and ONS 15310-MA use standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that the user needs to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

2.5.1 Alarm Characteristics

The ONS 15310-CL and ONS 15310-MA use standard alarm entities to identify what is causing trouble. All alarms stem from hardware, software, environment, or operator-originated problems whether or not they affect service. Current alarms for the network, CTC session, node, or card are listed in the Alarms tab. (In addition, cleared alarms are found in the History tab.)

2.5.2 Condition Characteristics

Conditions include any problem detected on an ONS 15310-CL or ONS 15310-MA shelf. They can include standing or transient notifications. A snapshot of all current raised, standing conditions on the network, node, or card can be retrieved in the CTC Conditions window or using TL1's set of RTRV-COND commands. (In addition, some but not all cleared conditions are found in the History tab.)

For a comprehensive list of all conditions, refer to the *Cisco SONET TL1 Command Guide*. For more information about transient conditions, see Chapter 3, “Transient Conditions.”

2.5.3 Severities

The ONS 15310-CL and ONS 15310-MA use Telcordia-devised standard severities for alarms and conditions: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) and Not Reported (NR). These are described as follows:

- A Critical (CR) alarm generally indicates severe, Service-Affecting (SA) trouble that needs immediate correction. Loss of traffic on an STS-1, which can hold 28 DS-1 circuits, would be a Critical (CR), Service-Affecting (SA) alarm.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network. For example, loss of traffic on more than five DS-1 circuits is Critical (CR), but loss of traffic on one to four DS-1 circuits is Major (MJ).
- Minor (MN) alarms generally are those that do not affect service. For example, the automatic protection switching (APS) byte failure (APSB) alarm indicates that line terminating equipment (LTE) detects a byte failure on the signal that could prevent traffic from properly executing a traffic switch.
- Not Alarmed (NA) conditions are information indicators, such as for the free-run synchronization state (FRNGSYNC) or a forced-switch to primary timing source event (FRCSWTOPRI). They could or could not require troubleshooting, as indicated in the entries.
- Not Reported (NR) conditions occur as a secondary result of another event. For example, the alarm indication signal (AIS), with severity NR, is inserted by a downstream node when an LOS (CR or MJ) alarm occurs upstream. These conditions do not in themselves require troubleshooting, but usually accompany primary alarms.

Severities can be customized for an entire network or for single nodes, from the network level down to the port level, by changing or downloading customized alarm profiles. These custom severities are subject to the standard severity-demoting rules given in Telcordia GR-474-CORE and shown in the 2.5.4 Alarm Hierarchy section. Procedures for customizing alarm severities are located in the "Manage Alarms" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

2.5.4 Alarm Hierarchy

All alarm, condition, and unreported event severities listed in this manual are default profile settings. However in situations when traffic is not lost, such as when the alarm occurs on protected ports or circuits, alarms having Critical (CR) or Major (MJ) default severities can be demoted to lower severities such as Minor (MN) or Non-Service-Affecting (NSA) as defined in Telcordia GR-474-CORE.

A path alarm can be demoted if a higher-ranking alarm is raised for the same object. For example, If a path trace identifier mismatch (TIM-P) is raised on a circuit path and then a loss of pointer on the path (LOP-P) is raised on the path, the LOP-P alarm stands and the TIM-P closes. The path alarm hierarchy used in the ONS 15310-CL and ONS 15310-MA systems is shown in Table 2-9.

Table 2-9 Path Alarm Hierarchy

Priority	Condition Type
Highest	AIS-P
—	LOP-P
—	UNEQ-P
Lowest	TIM-P

Facility (port) alarms also follow a hierarchy; lower-ranking alarms are closed by higher-ranking alarms. The facility alarm hierarchy used in the systems is shown in Table 2-10.

Table 2-10 Facility Alarm Hierarchy

Priority	Condition Type
Highest	LOS
—	LOF
—	AIS-L
—	SF-L
—	SD-L
—	RFI-L
—	TIM-S
—	AIS-P
—	LOP-P
—	SF-P
—	SD-P
—	UNEQ-P
—	TIM-P
Lowest	PLM-P

Near-end failures and far-end failures follow different hierarchies. Near-end failures stand according to whether they are for the entire signal (LOS, loss of frame alignment [LOF]), facility (AIS-L), path (AIS-P, etc.) or VT (AIS-V, etc.). The full hierarchy for near-end failures is shown in Table 2-11. This table is taken from Telcordia GR-253-CORE.

Table 2-11 Near-End Alarm Hierarchy

Priority	Condition Type
Highest	LOS
—	LOF
—	AIS-L
—	AIS-P[1]
—	LOP-P[2]
—	UNEQ-P
—	TIM-P
—	PLM-P
—	AIS-V[1]
—	LOP-V[2]
—	UNEQ-V

Table 2-11 Near-End Alarm Hierarchy

Priority	Condition Type
—	PLM-V
Lowest	DS-N AIS (if reported for outgoing DS-N signals)

1. Although it is not defined as a defect or failure, all-ones STS pointer relay is also higher priority than LOP-P. Similarly, all-ones VT pointer relay is higher priority than LOP-V.
2. LOP-P is also higher priority than the far-end failure RFI-P, which does not affect the detection of any near-end failures. Similarly, LOP-V is higher priority than RFI-V.

The far-end failure alarm hierarchy is shown in Table 2-12, as given in Telcordia GR-253-CORE.

Table 2-12 Far-End Alarm Hierarchy

Priority	Condition Type
Highest	RFI-L
—	RFI-P
Lowest	RFI-V

2.5.5 Service Effect

Service-Affecting (SA) alarms—those that interrupt service—could be Critical (CR), Major (MJ), or Minor (MN) severity alarms. Service-Affecting (SA) alarms indicate service is affected. Non-Service-Affecting (NSA) alarms always have a Minor (MN) default severity.

2.5.6 States

The State column on the Alarms or History tabs indicates the disposition of the alarm or condition as follows:

- A raised (R) event is one that is active.
- A cleared (C) event is one that is no longer active.
- A transient (T) event is one that is automatically raised and cleared in CTC during system changes such as user login, logout, loss of connection to node view, etc. Transient events do not require user action. These are listed in Chapter 3, "Transient Conditions."

2.6 Safety Summary

This section provides safety considerations designed to ensure safe operation of the ONS 15310-CL and ONS 15310-MA. Do not perform any procedures in this chapter unless you understand all safety precautions, practices, and warnings for the system equipment. Some troubleshooting procedures require installation or removal of cards; in these instances pay close attention to the following cautions and warnings.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Warning **Class 1 laser product.** Statement 1008

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.** Statement 43

Caution Hazardous voltage or energy could be present when the system is operating. Use caution when removing or installing cards.

2.7 Alarm Procedures

This section list alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severity, description, and troubleshooting procedure accompany each alarm and condition.

Note When you check the status of alarms for cards and ports, ensure that the alarm filter tool in the lower right corner of the GUI is not indented. When you are done checking for alarms, click the alarm filter tool again to turn filtering back on. For more information about alarm filtering, refer to the "Manage Alarms" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Note When checking alarms, ensure that alarm suppression is not enabled on the card or port. For more information about alarm suppression, refer to the "Manage Alarms" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

2.7.1 AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: BITS, DS1, DS3, FUDC

The Alarm Indication Signal (AIS) condition indicates that this node is detecting an alarm indication signal in the incoming signal SONET overhead.

Generally, an AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when the node sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolve the problem on the upstream node.

Clear the AIS Condition

Step 1 Determine whether there are alarms on the upstream nodes and equipment, especially the "LOS (OCN)" alarm on page 2-106, or if there are out-of-service (OOS,MT or OOS,DSBLD) ports.

Step 2 Clear the upstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.2 AIS-L

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: EC1, OCN

The AIS Line condition indicates that this node is detecting line-level AIS in the incoming signal. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

This condition can also be raised in conjunction with the "TIM-S" alarm on page 2-148 if AIS-L is enabled.

Clear the AIS-L Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-21.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.3 AIS-P

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: STSMON, STSTRM

The AIS Path condition means that this node is detecting AIS in the incoming path. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

Clear the AIS-P Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-21.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.4 AIS-V

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: VT-MON, VT-TERM

The AIS VT condition means that this node is detecting AIS in the incoming VT-level path.

See the "1.11.3 AIS-V on Unused 15310-CL-CTX Card VT Circuits" section on page 1-82 for more information.

Clear the AIS-V Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-21.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.5 ALS

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. That guide discusses all dense wavelength division multiplexing (DWDM) alarms.

2.7.6 APC-END

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. That guide discusses all DWDM alarms.

2.7.7 APSB

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The APS Channel Byte Failure alarm occurs when LTE detects protection switching byte failure or an invalid switching code in the incoming APS signal. Some older SONET nodes not manufactured by Cisco send invalid APS codes if they are configured in a 1+1 protection group with newer SONET nodes, such as the ONS 15310-CL and ONS 15310-MA. These invalid codes cause an APSB alarm on the ONS 15310-CL and ONS 15310-MA.

Clear the APSB Alarm

Step 1 Use an optical test set to examine the incoming SONET overhead to confirm inconsistent or invalid K bytes. For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the ONS 15310-CL and ONS 15310-MA.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.8 APSCDFLTK

The APSCDFLTK alarm is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.9 APSCINCON

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

An APS Inconsistent alarm means that an inconsistent APS byte is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15310-CL and ONS 15310-MA, to switch the SONET signal from a working to a protect path when necessary. An inconsistent APS code occurs when three consecutive frames contain nonidentical APS bytes, which in turn give the receiving equipment conflicting commands about switching.

Clear the APSCINCON Alarm

Step 1 Look for other alarms, especially the "LOS (OCN)" alarm on page 2-106,or the "LOF (OCN)" alarm on page 2-95 (or the "AIS" condition on page 2-20). Clearing these alarms clears the APSCINCON alarm.

Step 2 If an APSINCON alarm occurs with no other alarms, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.10 APSCM

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The APS Channel Mismatch alarm occurs when the ONS 15310-CL or ONS 15310-MA expects a working channel but receives a protect channel. In many cases, the working and protect channels are crossed and the protect channel is active. If the fibers are crossed and the working line is active, the alarm does not occur. The APSCM alarm occurs only on the system when bidirectional protection is used on OC-N ports in a 1+1 protection group configuration. The APSCM alarm does not occur in an optimized 1+1 protection configuration.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the APSCM Alarm

Step 1 Verify that the working-port channel fibers are physically connected directly to the adjoining node working-port channel fibers.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA system.

Step 2 If the fibers are correctly connected, verify that the protection-port channel fibers are physically connected directly to the adjoining node protection-port channel fibers.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.11 APSCNMIS

The APSCNMIS alarm is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.12 APSIMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The APS Invalid Mode alarm occurs if a 1+1 protection group is not properly configured at both nodes to send or receive the correct APS byte. A node that is either configured for no protection or is configured for unidirectional path switched ring (UPSR) protection does not send the right K2 APS byte anticipated by a system configured for 1+1 protection. The 1+1 protect port monitors the incoming K2 APS byte and raises this alarm if it does not receive the byte.

The alarm is superseded by an APSCM or APSMM alarm. It is not superseded by an AIS condition. It clears when the port receives a valid code for 10 ms.

Clear the APSIMP Alarm

Step 1 Check the configuration of the other node in the 1+1 protection group. If the far end is not configured for 1+1 protection, create the group. For procedures, refer to the "Turn Up Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 If the other end of the group is properly configured or the alarm does not clear after you have provisioned the group correctly, verify that the working ports and protect ports are cabled correctly.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA system.

Step 3 Ensure that both protect ports are configured for SONET.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.13 APS-INV-PRIM

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Optimized 1+1 APS Primary Facility condition occurs on OC-N ports in an optimized 1+1 protection system if the incoming primary section header does not indicate whether it is primary or secondary.

Note APS-INV-PRIM is an informational condition and does not require troubleshooting. If the APS switch is related to other alarms, troubleshoot these alarms as necessary using the procedures in this chapter.

2.7.14 APSMM

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

An APS Mode Mismatch failure alarm occurs on OC-3 ports when there is a mismatch of the protection switching schemes at the two ends of the span, such as being bidirectional at one end and unidirectional at the other. Each end of a span must be provisioned the same way: bidirectional and bidirectional or unidirectional and unidirectional.

If one end is provisioned for 1+1 protection switching and the other is provisioned for UPSR switching, an APSMM alarm occurs on the ONS 15310-CL or ONS 15310-MA that is provisioned for 1+1 protection switching.

Clear the APSMM Alarm

Step 1 For the reporting system, in node view verify the protection scheme provisioning by completing the following steps:

a. In node view, click the **Provisioning > Protection** tabs.

b. Click the 1+1 protection group configured for the OC-3 or OC-12 ports.

The chosen protection group is the protection group that is optically connected (with data communication channel [DCC] connectivity) to the far end.

Step 2 Click **Edit**.

Record whether the Bidirectional Switching check box is checked.

Step 3 Click **OK** in the Edit Protection Group dialog box.

Step 4 Log into the far-end node and verify that the OC-3 or OC-12 port 1+1 protection group is provisioned.

Step 5 Verify that the Bidirectional Switching check box matches the checked or unchecked condition of the box recorded in Step 1. If not, change it to match.

Step 6 Click **Apply**.

Step 7 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.15 APS-PRIM-FAC

Default Severity: Not Alarmed (NA)

Logical Objects: OCN

The Optimized 1+1 APS Invalid Primary Section condition occurs on OC-N ports in an optimized 1+1 protection system if there is an APS status switch between the primary and secondary facilities to identify which port is primary.

Note APS-PRIM-FAC is an informational condition and does not require troubleshooting. If the APS switch is related to other alarms, troubleshoot these alarms as necessary using the procedures in this chapter.

Clear the APS-PRIM-FAC Condition

Step 1 This condition clears when the card receives a valid primary section indication (1 or 2). Correct the selection if necessary.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.16 APS-PRIM-SEC-MISM

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Optimized 1+1 APS Primary Section Mismatch condition occurs on OC-N ports in an optimized 1+1 protection system if there is a mismatch between the primary section of the local node facility and the primary section of the remote-node facility.

Clear the APS-PRIM-SEC-MISM Alarm

Step 1 Ensure that the local node and remote-node ports are correctly provisioned the same way. For more information about optimized 1+1 configurations, refer to the "Turn Up Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.17 AS-CMD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BPLANE, CEMR, CE100T, CEMR, DS1, DS3, EC1, EQPT, ML100T, NE, OCN, PWR

DWDM Logical Objects: PPM, SHELF

The Alarms Suppressed by User Command condition applies to the network element (NE object), a single card, or a port on a card. It occurs when alarms are suppressed for that object and its subordinate objects. For example, suppressing alarms on a card also suppresses alarms on its ports.

Note For more information about suppressing alarms, refer to the "Manage Alarms" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Clear the AS-CMD Condition

Step 1 For all nodes, in node view, click the **Conditions** tab.

Step 2 Click **Retrieve**. If you have already retrieved conditions, look under the Object column and Eqpt Type column and note what entity the condition is reported against—such as a port, slot, or shelf.

- If the condition is reported against a slot and card, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and continue with Step 3.
- If the condition is reported against the NE object, go to Step 7.

Step 3 Determine whether alarms are suppressed for a port and if so, raise the suppressed alarms by completing the following steps:

a. Double-click the card to display the card view.

b. Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs and complete one of the following substeps:

- If the Suppress Alarms column check box is checked for a port row, deselect it and click **Apply**.
- If the Suppress Alarms column check box is not checked for a port row, click **View > Go to Previous View**.

Step 4 If the AS-CMD condition is reported for a card and not an individual port, in node view click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 5 Locate the row number for the reported card slot.

Step 6 Click the **Suppress Alarms** column check box to deselect the option for the card row.

Step 7 If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm, complete the following steps:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs if you have not already done so.

b. Click the **Suppress Alarms** check box located at the bottom of the window to deselect the option.

c. Click **Apply**.

Step 8 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.18 AS-MT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: CE100T, CEMR, DS1, DS3, EC1, EQPT, ML100T, OCN

DWDM Logical Objects: PPM, SHELF

The Alarms Suppressed for Maintenance Command condition applies to OC-3, OC-12, and electrical ports and occurs when a port is placed in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state for loopback testing operations.

Clear the AS-MT Condition

Step 1 Complete the "Clear an OC-N Port Facility or Terminal Loopback Circuit" procedure on page 2-165.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.19 AS-MT-OOG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The Alarms Suppressed on an Out-Of-Group VCAT Member alarm is raised on an STS or VT member of a virtual concatenated (VCAT) group whenever the member is in the IDLE (AS-MT-OOG) administrative state. This alarm can be raised when a member is initially added to a group. In IDLE (AS-MT-OOG) state, all other alarms for the STS or VT are suppressed.

The AS-MT-OOG alarm clears when an STS or VT member transitions to a different state from IDLE (AS-MT-OOG) or when it is removed completely from the VCAT group. It does not require troubleshooting unless it does not clear.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.20 AUD-LOG-LOSS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Audit Trail Log Loss condition occurs when the log is 100 percent full and the oldest entries are being replaced with new entries. The log capacity is 640 entries. The log must be off-loaded using the following procedure to make room for more entries.

Clear the AUD-LOG-LOSS Condition

Step 1 In node view, click the **Maintenance > Audit** tabs.

Step 2 Click **Retrieve**.

Step 3 Click **Archive**.

Step 4 In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.

Step 5 Enter a name in the **File Name** field.

You do not have to assign an extension to the file. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 6 Click **Save**.

The 640 entries are saved in this file. New entries continue with the next number in the sequence, rather than starting over.

Step 7 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.21 AUD-LOG-LOW

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Audit Trail Log Low condition occurs when the audit trail log is 80 percent full.

Note AUD-LOG-LOW is an informational condition and does not require troubleshooting.

2.7.22 AUTOLSROFF

The AUTOLSROFF ALARM is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.23 AUTORESET

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Automatic System Reset alarm occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot. AUTORESET typically clears after a card reboots (up to ten minutes).

Resets performed during a software upgrade also prompt the condition. This condition clears automatically when the card finishes resetting.

Clear the AUTORESET Alarm

Step 1 Determine whether additional alarms are present that could have triggered an automatic reset. If so, troubleshoot these alarms using the applicable section of this chapter.

Step 2 If the reporting card is an ML-100T-8, CE-MR-6, or CE-100T-8 card and automatically resets more than once a month with no apparent cause, complete the "Physically Replace a Card" procedure on page 2-163.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.24 AUTOSW-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, VT-MON

The Automatic Path Protection Switch Caused by an AIS condition indicates that automatic UPSR switching occurred because of an AIS condition. If the UPSR is configured for revertive switching, it reverts to the working path after the fault clears. The AIS also clears when the upstream trouble is cleared.

Note This condition is only reported if the path protection is set up for revertive switching.

Generally, an AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The AIS condition is raised by the receiving node on each input when the node sees the signal AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolve the problem on the upstream node.

Clear the AUTOSW-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-21.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.25 AUTOSW-LOP (STSMON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: STSMON

The Automatic Path Protection Switch Caused by LOP condition for the STS monitor (STSMON) condition indicates that automatic UPSR switching occurred because of the "LOP-P" alarm on page 2-98. If the UPSR is configured for revertive switching, it reverts to the working path after the fault clears.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-LOP (STSMON) Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-99.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.26 AUTOSW-LOP (VT-MON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: VT-MON

The AUTOSW-LOP alarm for the VT monitor (VT-MON) indicates that automatic UPSR switching occurred because of the "LOP-V" alarm on page 2-99. If the UPSR is configured for revertive switching, it reverts to the working path after the fault clears.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-LOP (VT-MON) Alarm

Step 1 Complete the "Clear the LOP-V Alarm" procedure on page 2-99.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.27 AUTOSW-PDI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, VT-MON

The Automatic Path Protection Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic UPSR switching occurred because of a "PDI-P" alarm on page 2-121. If the UPSR is configured for revertive switching, it reverts to the working path after the fault clears.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-PDI Condition

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-122.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.28 AUTOSW-SDBER

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, VT-MON

The Automatic Path Protection Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a "SD-P" condition on page 2-133 caused automatic UPSR protection switching to occur. If the path protection is configured for revertive switching, the path protection reverts to the working path when the SD-P is resolved.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-SDBER Condition

Step 1 Complete the "Clear the SD-P Condition" procedure on page 2-133.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.29 AUTOSW-SFBER

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, VT-MON

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a "SF-P" condition on page 2-135 caused automatic UPSR protection switching to occur. If the path protection is configured for revertive switching, the path protection reverts to the working path when the SF-P is resolved.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-SFBER Condition

Step 1 Complete the "Clear the SF-P Condition" procedure on page 2-135.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.30 AUTOSW-UNEQ (STSMON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: STSMON

The Automatic Path Protection Switch Caused by Unequipped condition indicates that an UNEQ alarm caused automatic UPSR protection switching to occur (see the "UNEQ-P" condition on page 2-151). If the UPSR is configured for revertive switching, it reverts to the working path after the fault clears.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-UNEQ (STSMON) Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-151.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.31 AUTOSW-UNEQ (VT-MON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: VT-MON

The automatic path protection switch caused by an unequipped condition (VT-MON) indicates that the "UNEQ-V" alarm on page 2-153 alarm caused automatic UPSR protection switching to occur. If the UPSR is configured for revertive switching, it reverts to the working path after the fault clears.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-UNEQ (VT-MON) Alarm

Step 1 Complete the "Clear the UNEQ-V Alarm" procedure on page 2-153.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.32 BAT-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: PWR

The Battery Fail alarm occurs when the power supply is not detected. This could be because the supply is removed or is not operational. The alarm does not distinguish between the individual power supplies, so onsite information about the conditions is necessary for troubleshooting.

Clear the BAT-FAIL Alarm

Step 1 At the site, determine which battery is not present or operational.

Step 2 Remove the power cable from the faulty supply. The "Install the Cisco ONS 15310-CL" chapter and the "Install the Cisco ONS 15310-MA" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* contains instructions for installing both AC (ONS 15310-CL only) and DC (ONS 15310-CL and ONS 15310-MA) power supply cables. To remove the cable, reverse the appropriate procedure.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.33 BERT-ENBL

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Object: DS1/DS3

The Bert Enabled alarm specifies that the bit error rate testing (BERT) feature is enabled.

2.7.34 BERT-SYNC-FAIL

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Object: DS1/DS3

The Bert Synchronization Fail alarm occurs when the errors injected by the Test Pattern Generator (TPG) reach the Test Pattern Monitor (TPM) and connectivity fails.

This alarm clears when TPG and TPM synchronize.

2.7.35 BKUPMEMP

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Primary Nonvolatile Backup Memory Failure alarm refers to a problem with the 15310-CL-CTX or CTX2500 card flash memory. The alarm occurs when the 15310-CL-CTX or CTX2500 card has one of four problems:

- Flash manager fails to format a flash partition.
- Flash manager fails to write a file to a flash partition.
- Problem at the driver level.
- Code volume fails cyclic redundancy checking (CRC, a method to verify for errors in data transmitted to the 15310-CL-CTX or CTX2500 card).

The BKUPMEMP alarm can also cause the "EQPT" alarm on page 2-57. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarms.

Clear the BKUPMEMP Alarm

Step 1 Verify that the controller card (15310-CL-CTX or CTX2500 card) is powered and enabled by confirming a lighted ACT LED on front of the system.

Step 2 Complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162.

Wait ten minutes to verify that the card you reset completely reboots. The ACT LED should be green.

Step 3 If the 15310-CL-CTX or CTX2500 card does not reboot successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447).

2.7.36 BLSROSYNC

The BLSROSYNC alarm is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.37 CARLOSS (CE100T, CEMR)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T, CEMR

The Carrier Loss alarm is raised on CE-Series cards in Mapper mode when the port is In-Service (IS) state and if there is no carrier signal. Circuit need not be present to raise the alarm. In releases prior to 6.01 the Carrier Loss alarm is raised on CE-100T-8 cards in Mapper mode when there is a circuit failure due to link integrity. It does not get raised when a user simply puts the port in the In-Service and Normal (IS-NR) service state.

Clear the CARLOSS (CE100T, CEMR) Alarm

Step 1 Verify that the fiber cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If the fiber cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device.

Step 3 Verify that the attached transmitting Ethernet device is operational. If not, troubleshoot the device.

Step 4 Verify that optical receive levels are within the normal range. The correct specifications are listed in the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 5 If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures.

Step 7 If the alarm does not clear, and link autonegotiation is enabled on the port but the autonegotiation process fails, the card turns off its transmitter laser and reports a CARLOSS alarm. If link autonegotiation has been enabled for the port, determine whether there are conditions that could cause autonegotiation to fail by completing the following steps:

- **a.** Confirm that the attached Ethernet device has autonegotiation enabled and is configured for compatibility with the asymmetric flow control on the card.
- **b.** Confirm that the attached Ethernet device configuration allows reception of flow control frames.

Step 8 If the alarm does not clear, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process restarts.)

Step 9 If the alarm does not clear and the "TPTFAIL" alarm on page 2-149 is also reported, complete the "Clear the TPTFAIL Alarm" procedure on page 2-149. If the TPTFAIL alarm is not raised, continue with the next step.

Note When the CARLOSS and the TPTFAIL alarms are reported, the reason for the condition could be the CE-Series card's end-to-end link integrity feature taking action on a remote failure indicated by the TPTFAIL alarm.

Step 10 If the TPTFAIL alarm was not raised, determine whether a terminal (inward) loopback has been provisioned on the port by completing the following steps:

a. In node view, click the card to go to card view.

b. Click the **Maintenance > Loopback tabs**.

c. If the service state is listed as OOS-MA,LPBK&MT, a loopback is provisioned. Go to Step 11.

Step 11 If a loopback was provisioned, complete the "Clear an Ethernet Card Loopback Circuit" procedure on page 2-166.

On the CE-100T-8, provisioning a terminal (inward) loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the CE-100T-8 card. Terminating the transmit laser could raise the CARLOSS alarm because the loopbacked CE-100T-8 port detects the termination. For more information about CE-100T-8 cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

If the port or card does not have a loopback condition, continue with Step 12.

Step 12 If a CARLOSS alarm repeatedly appears and clears, the reappearing alarm could be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps if the Ethernet circuit is part of a manual cross-connect by completing the following steps:

Note An Ethernet manual cross-connect is used when another vendor's equipment sits between ONS nodes, and the Open System Interconnection/Target Identifier Address Resolution Protocol (OSI/TARP)-based equipment does not allow tunneling of the TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

a. Right-click anywhere in the row of the CARLOSS alarm.

b. Right-click or left-click **Select Affected Circuits** in the shortcut menu that appears.

c. Record the information in the type and size columns of the highlighted circuit.

d. Examine the layout of your network and determine which node and card are hosting the Ethernet circuit at the other end of the Ethernet manual cross-connect using the following substeps:

- Log into the node at the other end of the Ethernet manual cross-connect.
- Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
- Click the **Circuits** tab.
- Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit connects the Ethernet port to an OC-N port at the same node.

e. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.

f. If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-164 and reconfigure the circuit with the correct circuit size. Refer to the "Create Circuits" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for detailed procedures to do this.

Step 13 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-163.

Step 14 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-163 for the Ethernet card.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 15 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.38 CARLOSS (EQPT)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: EQPT

A Carrier Loss on the LAN Equipment alarm generally occurs on OC-3 and OC-12 ports when the ONS 15310-CL or ONS 15310-MA and the workstation hosting CTC do not have a TCP/IP connection. The problem involves the LAN or data circuit used by the LAN (RJ-45) connector on the system. The CARLOSS alarm does not involve an Ethernet circuit connected to an Ethernet port. The problem is in the connection and not CTC or the node.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the CARLOSS (EQPT) Alarm

Step 1 If the reporting entity is a pluggable port module (PPM) port, confirm that the PPM is correctly configured by completing the following steps:

a. Double-click the controller card (15310-CL-CTX or CTX2500 card).

b. Click the **Provisioning > Pluggable Port Modules** tabs.

c. View the Pluggable Port Modules area port listing in the **Actual Eqpt Type** column and compare this with the contents of the Selected PPM area **Rate** column for the port.

d. If the rate does not match the actual equipment, you must delete and recreate the selected PPM. Select the PPM, click **Delete**, then click **Create** and choose the correct rate for the port rate.

Step 2 If the reporting port is an OC-3 or OC-12 port, verify connectivity by pinging the node that is reporting the alarm by completing the procedure in the "1.9.8 Verify Microsoft Windows PC Connection to the Node (Ping)" section on page 1-68.

Step 3 If the ping is successful, it demonstrates that an active TCP/IP connection exists. Restart CTC by completing the following steps:

a. Exit from CTC.

b. Reopen the browser.

c. Log into CTC.

Step 4 Using optical test equipment, verify that proper receive levels are achieved. (For specific procedures to use the test set equipment, consult the manufacturer.)

Step 5 Verify that the optical LAN cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 6 If the fiber cable is properly connected and attached to the port, verify that the cable connects the port to another Ethernet device and is not misconnected to an OC-3 or OC-12 port. For more information about fiber connections and terminations, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*. For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Step 7 If you are unable to establish connectivity, replace the fiber cable with a new known-good cable. To do this, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures.

Step 8 If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cable continuity using site practice, and troubleshoot any routers between the node and CTC.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.39 CARLOSS (ML100T)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: ML100T

A Carrier Loss alarm on an ML-100T-8 Ethernet card is the data equivalent of the "LOS (OCN)" alarm on page 2-106. The Ethernet port has lost its link and is not receiving a valid signal.

A CARLOSS alarm occurs when the Ethernet port has been configured from the Cisco IOS command line interface (CLI) as a no-shutdown port and one of the following problems also occurs:

- The cable is not properly connected to the near or far port.
- Autonegotiation is failing.
- The speed (10/100 ports only) is set incorrectly.

Note For information about provisioning ML-100T-8 Ethernet cards from the Cisco IOS interface, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the CARLOSS (ML100T) Alarm

Step 1 Verify that the LAN cable is properly connected and attached to the correct port on the ML-100T-8 card and on the peer Ethernet port. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 If the alarm does not clear, verify that autonegotiation is set properly on the ML-100T-8 card port and the peer Ethernet port.

Step 3 If the alarm does not clear, verify that the speed is set properly on the ML-100T-8 card port and the peer Ethernet port if you are using 10/100 ports.

Step 4 If the alarm does not clear, the Ethernet signal is not valid, but the transmitting device is operational, replace the LAN cable connecting the transmitting device to the Ethernet port.

Step 5 If the alarm does not clear, disable and reenable the Ethernet port by performing a "shutdown" and then a "no shutdown" on the Cisco IOS CLI as in the following example:

```
router(config)# shut

router(config)# no shut
```

This action restarts autonegotiation.

Step 6 If the alarm does not clear, complete the"1.2.1 Perform a Facility Loopback on a Source-Node Port" procedure on page 1-4 and test the loopback.

Step 7 If the problem persists with the loopback installed, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-163.

Step 8 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-163.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.40 CLDRESTART

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Cold Restart condition occurs when an Ethernet, E1-21-E3/DS3-3, E1-63-E3/DS3-3 or CTX-2500 card is reseated or replaced, or when the ONS 15310-CL or ONS 15310-MA power is initialized.

Clear the CLDRESTART Condition

Step 1 If the condition is raised on the controller card, it should clear after booting. If the condition is raised on an Ethernet card, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-163.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If the condition raised against an Ethernet, E1-21-E3/DS3-3, E1-63-E3/DS3-3 or CTX-2500 card does not clear, complete the "Physically Replace a Card" procedure on page 2-163 for the card.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.41 COMIOXC

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Input/Output Slot To Cross-Connect Communication Failure alarm is caused by the 15310-CL-CTX or CTX2500 card when there is a communication failure for a traffic slot.

Clear the COMIOXC Alarm

Step 1 Complete the "Soft- or Hard-Reset an Ethernet or Electrical Card in CTC" procedure on page 2-162 on the 15310-CL-CTX or CTX2500 card.

Caution Avoid soft-resetting multiple ONS 15310-MA cards at one time; doing so might cause an unexpected traffic hit.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT LED indicates an active card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.42 CONTBUS-CLK-A

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for ONS 15310-MA

SONET Logical Object: EQPT

An Inbound Interconnection Timing Control Bus 1 Failure alarm on the Slot 3 CTX2500 card occurs if the timing signal from the Slot 4 CTX2500 card has an error. If the Slot 3 CTX2500 card and all other cards on the shelf raise this alarm, the alarm processor on the Slot 4 CTX2500 card clears the alarm on the other cards and raises this alarm against the Slot 3 CTX2500 card only.

Clear the CONTBUS-CLK-A Alarm

Step 1 If a single traffic card is reporting the alarm and it is part of a path protection configration, complete the "Initiate a Force Switch for All Circuits on a Path Protection Span" procedure on page 2-160 procedure. If the traffic card is part of a 1+1 protection group, complete the "Clear a 1+1 Force or Manual Switch Command" procedure on page 2-158.

Step 2 Complete the appropriate procedure in the "2.10.3 Physical Card Reseating and Replacement" section on page 2-163 for the reporting card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Step 4 If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-157. If traffic was manually switched in a path protection configration, revert traffic to the original path by completing the "Clear an External Switching Command on a Path Protection Span" procedure on page 2-161.

2.7.43 CONTBUS-CLK-B

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for ONS 15310-MA

SONET Logical Object: EQPT

An Inbound Interconnection Timing Control Bus 1 Failure alarm on the Slot 4 CTX2500 card occurs if the timing signal from the Slot 3 CTX2500 card has an error. If the Slot 4 CTX2500 card and all other cards on the shelf raise this alarm, the alarm processor on the Slot 3 CTX2500 card clears the alarm on the other cards and raises this alarm against the Slot 4 CTX2500 card only.

Clear the CONTBUS-CLK-B Alarm

Step 1 If a single traffic port is reporting the alarm and it is part of a path protection configration, complete the "Initiate a Force Switch for All Circuits on a Path Protection Span" procedure on page 2-160. If the traffic port is part of a 1+1 protection group, complete the "Clear a 1+1 Force or Manual Switch Command" procedure on page 2-158.

Note If the active CTX2500 card is reporting the alarm, shelf control should already have switched off the card.

Step 2 Complete the appropriate procedure in the "2.10.3 Physical Card Reseating and Replacement" section on page 2-163 for the reporting card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Step 4 If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Clear a 1+1 Force or Manual Switch Command" procedure on page 2-158. If traffic was manually switched in a path protection configration, revert traffic to the original path by completing the "Clear an External Switching Command on a Path Protection Span" procedure on page 2-161.

2.7.44 CONTBUS-DISABLED

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The CONTBUS-DISABLED alarm occurs when an Ethernet card is defective upon insertion into the chassis or when a card that is already present in the chassis becomes defective. (That is, the card fails the enhanced cell bus verification test.) The alarm persists as long as the defective card remains in the chassis. When the card is removed, CONTBUS-DISABLED will remain raised for a one-minute wait time. This wait time is designed as a guard period so that the system can distinguish this outage from a briefer card reset communication outage.

If no card is reinserted into the original slot during the wait time, the alarm clears. After this time, a different, nondefective card (not the original card) should be inserted.

When CONTBUS-DISABLED is raised, no message-oriented communication is allowed to or from this Ethernet slot to the controller card (15310-CL-CTX or CTX2500 card), thus avoiding node communication failure.

Caution CONTBUS-DISABLED clears only when the faulty card is removed for one minute. If any card at all is reinserted before the one-minute guard period expires, the alarm does not clear.

CONTBUS-DISABLED overrides the IMPROPRMVL alarm during the one-minute wait period, but afterward IMPROPRMVL can be raised because it is no longer suppressed. IMPROPRMVL is raised after CONTBUS-DISABLED clears if the card is in the node database. If CONTBUS-DISABLED has cleared but IMPROPRMVL is still active, inserting a card will clear the IMPROPRMVL alarm.

For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the CONTBUS-DISABLED Alarm

Step 1 If the IMPROPRMVL alarm is raised, complete the "Physically Replace a Card" procedure on page 2-163. (For general information about card installation, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.)

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.45 CONTBUS-IO-A

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

A 15310-CL-CTX A or CTX2500 card to Shelf Slot Communication Failure alarm occurs when the cross-connecting card (in this platform, the controller card) has lost communication with another card slot in the shelf. The other card is identified by the Object column in the CTC alarm window.

Clear the CONTBUS-IO-A Alarm

Step 1 Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab and view the **Eqpt Type** column to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA (EQPT)" alarm on page 2-116 for the reporting card.

Step 2 Complete the "Soft- or Hard-Reset an Ethernet or Electrical Card in CTC" procedure on page 2-162.

Caution Avoid soft-resetting multiple ONS 15310-MA cards at one time; doing so might cause an unexpected traffic hit.

For LED behavior, see the "2.9.2 Typical Card LED Activity During Reset" section on page 2-156.

Wait ten minutes to verify that the card you reset completely reboots.

Step 3 If CONTBUS-IO-A is raised on more than one card at once, complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162.

Caution Avoid soft-resetting multiple ONS 15310-MA cards at one time; doing so might cause an unexpected traffic hit.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT LED indicates an active card.

Step 5 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447).

2.7.46 CONTBUS-IO-B

The CONTBUS-IO-B alarm is not used in the Cisco ONS 15310 platforms in this release. It is reserved for development.

2.7.47 CTNEQPT-PBPROT

Default Severity: Critical (CR), Service-Affecting (SA) for ONS 15310-MA

SONET Logical Object: EQPT

The Interconnection Equipment Failure Protect Cross-Connect Card Payload Bus Alarm indicates a failure of the main payload between the protect CTX2500 card Slot 4 cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card and the reporting traffic card, or the controller card and the backplane.

Note This alarm automatically raises and clears when the Slot 4 controller card is reseated.

Clear the CTNEQPT-PBPROT Alarm

Step 1 If all traffic cards show CTNEQPT-PBPROT alarm, complete the following steps:

a. Complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-163 for the standby CTX2500 card.

b. If the reseat fails to clear the alarm, complete the "Physically Replace a Card" alarm on page 2-163 procedure for the standby CTX2500 card.

Caution Do not physically reseat an active CTX2500 card. Doing so disrupts traffic.

Step 2 If not all cards show the alarm, perform a CTC reset on the standby CTX2500 card. Complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162 procedure.

Caution Avoid soft-resetting multiple ONS 15310-MA cards at one time; doing so might cause an unexpected traffic hit.

For the LED behavior, see the "2.9.2 Typical Card LED Activity During Reset" procedure on page 2-156.

Step 3 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

If the cross-connect reset is not complete and error-free or if the CTX2500 card reboots automatically, call Cisco TAC (1 800 553-2447).

Step 4 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-163 procedure for the standby Ethernet card.

Step 5 Determine whether the card is an active card or standby card in a protection group. Click the node view **Maintenance > Protection** tabs, then click the protection group. The cards and their status are displayed in the list.

Step 6 If the reporting traffic card is the active card in the protection group, complete the "Initiate an ONS 15310-MA 1:1 Card Switch Command" procedure on page 2-159. After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.

Step 7 Complete the "Soft- or Hard-Reset an Ethernet or Electrical Card in CTC" procedure on page 2-162 for the reporting card.

Caution Avoid soft-resetting multiple ONS 15310-MA cards at one time; doing so might cause an unexpected traffic hit.

For the LED behavior, see the "2.9.2 Typical Card LED Activity During Reset" section on page 2-156.

Step 8 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 9 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-163 procedure for the standby Ethernet card.

Step 10 Complete the "Initiate an ONS 15310-MA 1:1 Card Switch Command" procedure on page 2-159 to switch traffic back.

Step 11 If the alarm does not clear, complete the "Physically Replace a Card" section on page 2-163 procedure for the reporting traffic card.

Step 12 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.7.48 CTNEQPT-PBWORK

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Interconnection Equipment Failure Working 15310-CL-CTX or CTX2500 card Payload Bus alarm indicates a failure in the main payload bus between the 15310-CL-CTX or CTX2500 card and the reporting Ethernet card. The controller card and the Ethernet or electrical card are no longer communicating.

Clear the CTNEQPT-PBWORK Alarm

Step 1 If the alarm is reported against the 15310-CL-CTX or CTX2500 card, go to Step 4. If the Ethernet or electrical traffic card shows the CTNEEQPT-PBWORK alarm, complete the "Soft- or Hard-Reset an Ethernet or Electrical Card in CTC" procedure on page 2-162 for the card.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT LED indicates an active card.

Step 3 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-163.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.49 DATA-CRC;

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T, ML100T

The data cyclic redundancy check (CRC) Bad Packet Count Exceeds Threshold alarm indicates that Cisco proprietary ring-wrapping (RPR) has been triggered for an ML-100T-8 or CE-100T-8 card in high-level data link (HDLC) mode, but no SONET or data-level alarm is raised along with RPRW, page 129, to indicate the failure.

In a typical scenario that triggers Cisco proprietary RPR protection, the errored node raises RPRW, and SONET or data errors such as TPTFAIL, page 149. If, however, a packet-over-SONET (POS) port is placed in down administrative state, the card will raise an RPRW without raising any SONET B3 bit alarms or data alarms. The DATA-CRC alarm accompanies this instance of RPRW to indicate the signal interruption.

Note This alarm is used only in the Cisco ONS 15310-MA platform in this release.

Clear the DATA-CRC Alarm

Step 1 Determine whether the "RPRW" alarm on page 2-129, is raised on the ring. If so, clear it using the appropriate trouble-clearing procedure in this chapter.

Step 2 If the DATA-CRC alarm does not clear, check whether the alarmed card POS port is in the Down administrative state:

a. Double-click the ML-100T-8 or CE-100T-8 card to display the card view.

b. Click the **Provisioning > POS Ports** tabs.

c. View the port's setting in the Admin State column. If it is Down, verify that both POS ports are properly configured. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide* for configuration information.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.50 DATAFLT

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Software Data Integrity Fault alarm occurs when the 15310-CL-CTX card or CTX2500 card exceeds its flash memory capacity.

Clear the DATAFLT Alarm

Step 1 Complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162.

Caution Avoid soft-resetting multiple ONS 15310-MA cards at one time; doing so might cause an unexpected traffic hit.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.51 DBOSYNC

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: NE

The Standby Database Out Of Synchronization alarm applies to the ONS 15310-MA platform and occurs when the standby CTX2500 card database does not synchronize with the active database on the active CTX2500 card.

Caution If you reset the active CTX2500 card while this alarm is raised, you will lose current provisioning.

Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active CTX2500 card database. Refer to the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures.

Step 2 Make a minor provisioning change to the active database to see if applying a provisioning change clears the alarm:

a. In node view, click the **Provisioning > General > General** tabs.

b. In the Description field, make a small change such as adding a period to the existing entry.

The change causes a database write but does not affect the node state. The write could take up to a minute.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.52 DISCONNECTED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: SYSTEM

The Disconnected alarm is raised when CTC has been disconnected from the node. The alarm is cleared when CTC is reconnected to the node.

Clear the DISCONNECTED Alarm

Step 1 Restart the CTC application.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.53 DS3-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The DS-3 Frame Format Mismatch condition indicates that a line type format mismatch on a signal received on the DS-3 port of a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card. The condition occurs when the provisioned line type and incoming signal frame format type do no match. For example, if the line type for a DS-3 port is set to C Bit and the incoming signal line type is detected as M13, then the port reports a DS3-MISM condition.

Clear the DS3-MISM Condition

Step 1 In node view, double-click the CTX2500 card to display the card view.

Step 2 Click the **Provisioning > DS3 > Line** tabs.

Step 3 For the row on the appropriate port, verify that the Line Type column is set to match the expected incoming signal (C bit or M13).

Step 4 If the Line Type field does not match the expected incoming signal, select the correct Line Type in the drop-down list.

Step 5 Click **Apply**.

Step 6 If the condition does not clear after the user verifies that the provisioned line type matches the expected incoming signal, use an optical test set to verify that the actual signal coming into the node matches the expected incoming signal. For specific procedures to use the test set equipment, consult the manufacturer.

Step 7 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.54 DUP-IPADDR

Default Severity: Minor (MN), Non-Service Affecting (NSA)

SONET Logical Object: NE

The Duplicate IP Address alarm indicates that the alarmed node IP address is already in use within the same DCC area. When this happens, CTC no longer reliably connects to either node. Depending on how the packets are routed, CTC could connect to either node (having the same IP address). If CTC has connected to both nodes before they shared the same address, it has two distinct NodeModel instances (keyed by the node ID portion of the MAC address).

Clear the DUP-IPADDR Alarm

Step 1 Isolate the alarmed node from the other node having the same address by completing the following steps:

- **a.** Connect to the alarmed node using the Craft port on the chassis.
- **b.** Begin a CTC session.
- **c.** In the login dialog box, uncheck the **Network Discovery** check box.

Step 2 In node view, click the **Provisioning > Network > General** tabs.

Step 3 In the IP Address field, change the IP address to a unique number.

Step 4 Click **Apply**.

Step 5 Restart any CTC sessions that are logged into either of the formerly duplicated node IDs. (For procedures to log in or log out, refer to the "Set Up PC and Log Into the GUI" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.)

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.55 DUP-NODENAME

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Duplicate Node Name alarm indicates that the alarmed node alphanumeric name is already being used within the same DCC area.

Clear the DUP-NODENAME Alarm

Step 1 In node view, click the **Provisioning > General** tabs.

Step 2 In the Node Name/TID field, enter a unique name for the node.

Step 3 Click **Apply**.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.56 DUP-SHELF-ID

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. That guide discusses all DWDM alarms.

2.7.57 EHIBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: PWR

The Extreme High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the extreme high power threshold.

This preset value is approximately -56 VDC for the Cisco ONS 15310-CL hardware platforms versions 800-24012-08 and before and approximately -58 VDC for versions 800-24012-09 and later. Also, the extreme high voltage batter value is approximately -54 VDC for CTX version of the Cisco ONS 15310-MA hardware versions 800-23879-04 and before and is approximately -58 VDC for CTX version of the Cisco ONS 15310-MA hardware version 800-23879-05 and later. The alarm is raised until the voltage remains under the threshold for 120 seconds.

Clear the EHIBATVG Alarm

Step 1 The problem is external to the ONS 15310-CL or ONS 15310-MA. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.58 ELWBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: PWR

The Extreme Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the extreme low power threshold. This threshold has a preset value of –40 VDC and is not user-provisionable. The alarm remains raised until the voltage remains over the threshold for 120 seconds.

Clear the ELWBATVG Alarm

Step 1 The problem is external to the ONS 15310-CL or ONS 15310-MA. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.59 ENCAP-MISMATCH-P

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: STSTRM

The Encapsulation C2 Byte Mismatch Path alarm applies to the ML-100T-8 Ethernet card. It occurs when the first three following conditions are met and one of the last two is false:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped unspecified).
- The received C2 byte is not 0x01 (equipped unspecified).

(This is in contrast to the "PLM-P" alarm on page 2-122, which must meet all five criteria.) For an ENCAP-MISMATCH-P alarm to be raised, there is a mismatch between the received and expected C2 byte, with either the expected byte or received byte value being 0x01.

For example, an ENCAP-MISMATCH-P alarm is raised if a circuit created between two ML-100T-8 cards has generic framing procedure (GFP) framing provisioned on one end and high-level data link control (HDLC) framing with LEX encapsulation provisioned on the other. The GFP-framing card transmits and expects a C2 byte of 0x1B, while the HDLC-framing card transmits and expects a C2 byte of 0x01.

A mismatch between the transmit and receive ports on any of the following parameters can cause the alarm:

- Mode (HDLC, GFP-F)
- Encapsulation (LEX, HDLC, PPP)
- CRC size (16 or 32)
- Scrambling state (on or off)

This alarm is demoted by PLM-P or PLM-V.

Note By default, an ENCAP-MISMATCH-P alarm causes an ML-100T-8 card data link to go down. This behavior can be modified using the Cisco IOS command line interface (CLI) command **no pos trigger defect encap**.

Note For more information about the ML-100T-8 Ethernet card, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide.*

Clear the ENCAP-MISMATCH-P Alarm

Step 1 Ensure that the correct line type is in use on the receive card by completing the following steps:

a. In node view, double-click the receive ML-100T-8 card to display the card view.

b. Click the **Provisioning > Card** tabs.

c. In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 2 Ensure that the correct line type is in use on the transmit card and that it is identical to the receiving card by completing the following steps:

a. In node view, double-click the transmit ML-100T-8 card to display the card view.

b. Click the **Provisioning > Card** tabs.

c. In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 3 If the alarm does not clear, use the CLI to ensure that the remaining settings are correctly configured on the ML-100T-8 card:

- Encapsulation
- CRC size
- Scrambling state

To open the interface, click the **IOS** tab and click **Open IOS Command Line Interface (CLI)**. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide* entries on all three of these topics to obtain the full configuration command sequences.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.60 EOC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The SONET DCC Termination Failure alarm occurs when the ONS 15310-CL or ONS 15310-MA loses its DCC. The section data communication channel (SDCC) overhead consists of three bytes, D1 through D3, in the SONET overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The node uses the DCC on the SONET section layer to communicate network management information.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note If a circuit shows a partial state when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC Alarm

Step 1 If the "LOS (OCN)" alarm on page 2-106 is also reported, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-106.

Step 2 If the "SF-L" condition on page 2-134 is reported, complete the "Clear the SF-L Condition" procedure on page 2-135.

Step 3 If the alarm does not clear on the reporting node, ensure that the physical connections between the ports and that the fiber-optic cables are configured to carry SDCC traffic. If they are not, correct them. For more information about fiber connections and terminations, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

If the physical connections are correct and configured to carry DCC traffic, verify that both ends of the fiber span have in-service (IS-NR) ports. Verify that the ACT LED is green.

Step 4 When the LED on the controller card (15310-CL-CTX or CTX2500 card) is green, complete the "Verify or Create Node DCC Terminations" procedure on page 2-164 to ensure that the DCC is provisioned for the ports at both ends of the fiber span.

Step 5 Repeat Step 4 at the adjacent nodes.

Step 6 If DCC is provisioned for the ends of the span, verify that the port is active and in service by completing the following steps:

a. In node view, double-click the 15310-CL-CTX or CTX2500 card to display the card view.

b. Click the **Provisioning > Optical > Line** tabs.

c. Confirm that the OC-3 or OC-12 port shows a green LED.

   A green ACT LED indicates an active card.

d. Verify that the Admin State column lists the port as **IS**.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and click **IS** from the drop-down list. Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Step 7 For all nodes, if the card is in service, use an optical test set to determine whether signal failures are present on fiber terminations. For specific procedures to use the test set equipment, consult the manufacturer.

Caution Using an optical test set disrupts service on the OC-N port. It could be necessary to manually switch traffic carrying circuits over a protection path. See the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 for commonly used switching procedures.

Step 8 If no signal failures exist on terminations, measure power levels to verify that the loss is within the parameters of the receiver. Refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for card power levels.

Step 9 If loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162.

Caution Avoid soft-resetting multiple ONS 15310-MA cards at one time; doing so might cause an unexpected traffic hit.

Wait ten minutes to verify that the card you reset completely reboots.

Step 11 If the controller card reset does not clear the alarm, delete the problematic SDCC termination by completing the following steps:

a. From card view, click **View > Go to Previous View** if you have not already done so.

b. Click the **Provisioning > Comm Channels > SDCC** tabs.

c. Highlight the problematic DCC termination.

d. Click **Delete**.

e. Click **Yes** in the Confirmation Dialog box.

Step 12 Recreate the SDCC termination. Refer to the "Turn Up Network" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures.

Step 13 Verify that both ends of the DCC have been recreated at the optical ports.

Step 14 If the alarm has not cleared, call Cisco TAC (1-800-553-2447).

2.7.61 EOC-L

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Line DCC (LDCC) Termination Failure alarm occurs when the ONS 15310-CL or ONS 15310-MA loses its LDCC termination. The LDCC consists of nine bytes, D4 through D12, that convey information about OAM&P and network management information in the SONET overhead.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note If a circuit shows an incomplete state when the EOC or EOC-L alarm is raised, it occurs when the logical circuit is in place. The circuit is able to carry traffic when the DCC termination issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC-L Alarm

Step 1 Complete the "Clear the EOC Alarm" procedure on page 2-55.

Step 2 If the alarm has not cleared, call Cisco TAC (1-800-553-2447).

2.7.62 EQPT

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

DWDM Logical Object: PPM

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a BKUPMEMP alarm, refer to the "BKUPMEMP" alarm on page 2-36. The BKUPMEMP procedure also clears the EQPT alarm.

Clear the EQPT Alarm

Step 1 If traffic is active on the alarmed port, you might need to switch traffic away from it. See the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 for commonly used traffic-switching procedures.

Step 2 Complete the "Soft- or Hard-Reset an Ethernet or Electrical Card in CTC" procedure on page 2-162 for the reporting card.

Caution Avoid soft-resetting multiple ONS 15310-MA cards at one time; doing so might cause an unexpected traffic hit.

For the LED behavior, see the "2.9.2 Typical Card LED Activity During Reset" section on page 2-156.

Step 3 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-163 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 4 If the physical reseat of the card fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-163 for the reporting card.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.63 EQPT-MISS

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: FAN

The Replaceable Equipment or Unit Missing alarm is reported against the fan tray within the ONS 15310-CL or ONS 15310-MA. It indicates that the fan is not operational, or that the ONS 15310-MA fan tray is not present. For an ONS 15310-CL, this alarm is not user-serviceable. For the ONS 15310-MA, complete the fan tray replacement procedure located in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.64 ERFI-P-CONN

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Three-Bit (Enhanced) Remote Failure Indication (ERFI) Path Connectivity condition is triggered on DS-1, DS-3, or VT circuits when the "UNEQ-P" alarm on page 2-151 and the "TIM-P" alarm on page 2-148 are raised on the transmission signal.

Clear the ERFI-P-CONN Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-151 and the "Clear the TIM-P Alarm" procedure on page 2-148. This should clear the ERFI condition.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.65 ERFI-P-PAYLD

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Three-Bit ERFI Path Payload condition is triggered on DS-1, DS-3, or VT circuits when the "PLM-P" alarm on page 2-122 alarm is raised on the transmission signal.

Clear the ERFI-P-PAYLD Condition

Step 1 Complete the "Clear the PLM-P Alarm" procedure on page 2-123. This should clear the ERFI condition.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.66 ERROR-CONFIG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Error in Startup Configuration alarm applies to the ML-100T-8 Ethernet cards. These cards process startup configuration files line by line. If one or more lines cannot be executed, the error causes the ERROR-CONFIG alarm. ERROR-CONFIG is not caused by hardware failure.

The typical reasons for an errored startup file are:

- The user stored the configuration for one type of ML-100T-8 Ethernet card in the database and then installed another type in its slot.
- The configuration file contained a syntax error.

Note For information about provisioning the ML-100T-8 Ethernet cards from the Cisco IOS interface, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide.*

Clear the ERROR-CONFIG Alarm

Step 1 If the ML-100T-8 Ethernet configuration is different from the actual installation, create the correct startup configuration based upon the installation.

Consult the ML-100T-8 POS provisioning parameters for the card and POS ports in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Step 2 Upload the configuration file to the controller card (15310-CL-CTX or CTX2500 card) by completing the following steps:

a. In node view, right-click the ML-100T-8 Ethernet card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > TCC** and navigate to the file location in the Open dialog box.

Step 3 Complete the "Soft- or Hard-Reset an Ethernet or Electrical Card in CTC" procedure on page 2-162.

Caution Avoid soft-resetting multiple ONS 15310-MA cards at one time; doing so might cause an unexpected traffic hit.

Step 4 If the alarm does not clear or if your configuration file was correct according to the installed card, start a Cisco IOS CLI for the card by completing the following steps:

a. Right-click the ML-100T-8 Ethernet card graphic in node view.

b. Choose **Open IOS Connection** from the shortcut menu.

Note "Open IOS Connection" is not available unless the ML-100T-8 Ethernet card is physically installed in the shelf.

Follow the card provisioning instructions in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide* to correct the errored configuration file line.

Step 5 Execute the following CLI command:

```
copy run start
```

The command copies the new card configuration into the database and clears the alarm.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.67 ETH-LINKLOSS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Rear Panel Ethernet Link Removed condition, if enabled in the network defaults, is raised under the following conditions:

- The node.network.general.AlarmMissingBackplaneLAN field in NE default is enabled.
- The node is configured as a gateway network element (GNE).
- The LAN cable is removed.

For more information about Ethernet operation in the ONS 15310-CL or ONS 15310-MA, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the ETH-LINKLOSS Condition

Step 1 To clear this condition, reconnect the LAN cable on the front of the node.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.68 EXCCOL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Excess Collisions on the LAN alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15310-CL or ONS 15310-MA and CTC could be affected. The network management LAN is the data network connecting the workstation running the CTC software to the controller card. The problem causing the alarm is external to the node.

Troubleshoot the network management LAN connected to the ONS 15310-CL or ONS 15310-MA for excess collisions. You might need to contact the system administrator of the network management LAN to accomplish the following steps.

Clear the EXCCOL Alarm

Step 1 Verify that the network device port connected to the ONS 15310-CL or ONS 15310-MA has a flow rate set to 10 MB, half-duplex.

Step 2 If the port has the correct flow rate and duplex setting, troubleshoot the network device connected to the node and the network management LAN.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.69 EXT

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: ENVALRM

A Failure Detected External to the NE alarm occurs because an environmental alarm is present. For example, a door could be open or flooding could have occurred.

Clear the EXT Alarm

Step 1 Follow your standard operating procedure to remedy environmental conditions that cause alarms. The alarm clears when the situation is remedied.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.70 FAILTOSW

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Failure to Switch to Protection Facility condition occurs when a working or protect optical facility switches to its companion port by using a MANUAL command. For example, if you attempt to manually switch traffic from an unused protect port to an in-service working port, the switch will fail (because traffic is already present on the working port) and you will see the FAILTOSW condition.

Clear the FAILTOSW Condition

Step 1 Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the port and clears the FAILTOSW.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.71 FAILTOSW-PATH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, VTMON

The Fail to Switch to Protection Path condition occurs when the circuit does not switch from the working path to the protect path on a path protection configration. Common causes of the FAILTOSW-PATH condition include a missing or defective protect port, a lockout set on one of the UPSR nodes, or path-level alarms that would cause a UPSR switch to fail including the "AIS-P" condition on page 2-21, the "LOP-P" alarm on page 2-98, the "SD-P" condition on page 2-133, the "SF-P" condition on page 2-135, and the "UNEQ-P" alarm on page 2-151.

The "LOF (OCN)" alarm on page 2-95, the "LOS (OCN)" alarm on page 2-106, the "SD-L" condition on page 2-132, or the "SF-L" condition on page 2-134 can also occur on the failed path.

Clear the FAILTOSW-PATH Condition in a Path Protection Configuration

Step 1 Look up and clear the higher priority alarm. If the "AIS-P" condition on page 2-21, the "LOP-P" alarm on page 2-98, the "UNEQ-P" alarm on page 2-151, the "SF-P" condition on page 2-135, the "SD-P" condition on page 2-133, the "LOF (OCN)" alarm on page 2-95, the "LOS (OCN)" alarm on page 2-106, the "SD-L" condition on page 2-132, or the "SF-L" condition on page 2-134 are also occurring on the reporting port, complete the applicable alarm clearing procedure.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.72 FAN

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: FAN

The Fan Failure alarm indicates a problem with the internal fan of the ONS 15310-CL or ONS 15310-MA. When the fan is not fully functional, the temperature of the node can rise above its normal operating range.

The Fan Failure alarm is also reported against the fan unit located inside the ONS 15310-CL or ONS 15310-MA if only one power source is connected to the chassis, or if any fuse blows.

This alarm is not user-serviceable. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a Service-Affecting (SA) problem (1-800-553-2447).

2.7.73 FAN-DEGRADE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

SONET Logical Object: FAN

The Partial Fan Failure Speed Control Degradation alarm occurs if fan speed for one of the fans in the ONS 15310-CL or ONS 15310-MA shelf falls under 500 RPM when read by a tachometry counter.

For an ONS 15310-CL, this alarm is not user-serviceable. For an ONS 15310-MA, refer to the fan tray replacement procedure located in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.74 FE-AIS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far-End AIS condition occurs when an AIS has occurred at the far-end node. FE-AIS usually occurs in conjunction with a downstream LOS alarm (see the "LOS (OCN)" alarm on page 2-106).

Generally, an AIS is a special SONET signal that tells the receiving node that the sending node has no valid signal available to send. AIS is not considered an error. The AIS condition is raised by the receiving node on each input when it detects the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolve the problem on the upstream node.

Clear the FE-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-21.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.75 FE-DS1-MULTLOS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far-End Multiple DS-1 LOS Detected condition occurs when multiple DS-1 signals are lost on a far-end 15310-CL-CTX, ONS 15310-MA DS1-28/DS3-EC1-3, or ONS 15310-MA DS1-84/DS3-EC1-3 DS-1 port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-MULTLOS condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-MULTLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the port reporting the FE condition.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.76 FE-DS1-NSA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End DS-1 Equipment Failure Non-Service-Affecting (NSA) condition occurs when a far-end 15310-CL-CTX, ONS 15310-MA DS1-28/DS3-EC1-3, or ONS 15310-MA DS1-84/DS3-EC1-3 DS-1 port equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

Clear the FE-DS1-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the port reporting the FE alarm.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.77 FE-DS1-SA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End DS-1 Equipment Failure Service Affecting condition occurs when there is a far-end equipment failure on a 15310-CL-CTX, ONS 15310-MA DS1-28/DS3-EC1-3, or ONS 15310-MA DS1-84/DS3-EC1-3 DS-1 port that affects service because traffic is unable to switch to the protect port.

Clear the FE-DS1-SA Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the port reporting the FE alarm.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.78 FE-DS1-SNGLLOS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far-End Single DS-1 LOS condition occurs when a single DS-1 signal is lost on a far-end 15310-CL-CTX, ONS 15310-MA DS1-28/DS3-EC1-3, or ONS 15310-MA DS1-84/DS3-EC1-3 DS-1 port (within a DS3). Signal loss also causes the "LOS (OCN)" alarm on page 2-106.

Clear the FE-DS1-SNGLLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.79 FE-DS3-NSA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End DS-3 Equipment Failure Non-Service-Affecting (SA) condition occurs when a far-end 15310-CL-CTX, ONS 15310-MA DS1-28/DS3-EC1-3, or ONS 15310-MA DS1-84/DS3-EC1-3 DS-1 port equipment failure occurs in C-bit line type mode, but does not affect service because the port is protected and traffic is able to switch to the protect port.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting FE-DS3-NSA alarm. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS3-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and port link directly to the card reporting the FE alarm.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.80 FE-DS3-SA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End DS-3 Equipment Failure Service-Affecting condition occurs when there is a far-end equipment failure on a 15310-CL-CTX, ONS 15310-MA DS1-28/DS3-EC1-3, or ONS 15310-MA DS1-84/DS3-EC1-3 DS-1 port that affects service because traffic is unable to switch to the protect port.

Clear the FE-DS3-SA Condition

Step 1 To troubleshoot an FE condition, determine which node and port link directly to the card reporting the FE alarm.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.81 FE-EQPT-NSA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End Common Equipment Failure condition occurs when a Non-Service-Affecting (NSA) equipment failure is detected on a far-end 15310-CL-CTX, ONS 15310-MA DS1-28/DS3-EC1-3, or ONS 15310-MA DS1-84/DS3-EC1-3 DS-1 port.

Clear the FE-EQPT-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and port link directly to the card reporting the FE condition.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.82 FE-FRCDWKSWBK-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far End Forced Switch Back to Working—Span condition is raised on a far-end 1+1 protect port when it is Force switched to the working port.

Note WKSWBK-type conditions apply only to nonrevertive circuits.

Clear the FE-FRCDWKSWBK-SPAN Condition

Step 1 Complete the "Clear a 1+1 Force or Manual Switch Command" section on page 2-158 for the far-end port.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.83 FE-FRCDWKSWPR-SPAN

The FE-FRCDWKSWPR-SPAN condition is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.84 FE-IDLE

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End Idle condition occurs when a far-end node detects an idle far-end 15310-CL-CTX, ONS 15310-MA DS1-28/DS3-EC1-3, or ONS 15310-MA DS1-84/DS3-EC1-3 card DS-3 signal in C-bit line type mode.

Clear the FE-IDLE Condition

Step 1 To troubleshoot the FE condition, determine which node and port link directly to the card reporting the FE condition.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Clear the main alarm by clearing the protection switch. See the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 for commonly used traffic-switching procedures.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.85 FE-LOCKOUTOFPR-SPAN

The FE-LOCKOUTOFPR-SPAN condition is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.86 FE-LOF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End LOF condition occurs when a far-end node reports the "LOF (DS3)" alarm on page 2-94 in C-bit line type mode.

Clear the FE-LOF Condition

Step 1 To troubleshoot an FE condition, determine which node and port link directly to the card reporting the FE condition.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Complete the "Clear the LOF (DS1) Alarm" procedure on page 2-94. It also applies to FE-LOF.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.87 FE-LOS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End LOS condition occurs in C-bit line type mode when a far-end node reports the "LOS (DS3)" alarm on page 2-102.

Clear the FE-LOS Condition

Step 1 To troubleshoot the FE condition, determine which node and port link directly to the card or port reporting the FE condition.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Complete the "Clear the LOS (DS1) Alarm" procedure on page 2-101.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.88 FE-MANWKSWBK-SPAN

The FE-MANWKSWBK-SPAN condition is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.89 FE-MANWKSWPR-SPAN

The FE-MANWKSWPR-SPAN condition is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.90 FEPRLF

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far End Protection Line Failure alarm occurs when an APS channel "SF-L" condition on page 2-134 occurs on the protect port coming into the node.

Note The FEPRLF alarm occurs when bidirectional protection is used on optical ports in a 1+1 protection group configuration.

Clear the FEPRLF Alarm

Step 1 To troubleshoot the FE alarm, determine which node and port link directly to the port reporting the FE alarm.

Step 2 Log into the node that links directly to the port reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for instructions.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.91 FORCED-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, VT-MON

The Force Switch Request on Facility or Port condition occurs when you enter the Force command on a port to force traffic from a working port to a protect port or protection span (or from a protect port to a working port or span). You do not need to clear the condition if you want the Force switch to remain.

Clear the FORCED-REQ Condition

Step 1 Complete the "Clear a 1+1 Force or Manual Switch Command" procedure on page 2-158.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.92 FORCED-REQ-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Force Switch Request Span condition applies to optical trunk cards in spans when the Force Span command is applied to a span to force traffic from working to protect or from protect to working. This condition appears on the network view Alarms, Conditions, and History tabs. The port where the Force Span command was applied is marked with an "F" on the network view detailed circuit map.

This condition can also be raised in 1+1 facility protection groups. If traffic is present on a working port and you use the Force command to prevent it from switching to the protect port (indicated by "FORCED TO WORKING"), FORCED-REQ-SPAN indicates this force switch. In this case, the force is affecting not only the facility, but the span.

Clear the FORCED-REQ-SPAN Condition

Step 1 Complete the "Clear an External Switching Command on a Path Protection Span" procedure on page 2-161.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.93 FP-LINK-LOSS

The FP-LINK-LOSS alarm is not used in the Cisco ONS 15310 platforms in this release. It is reserved for development.

2.7.94 FRCDSWTOINT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE-SREF

The Force Switch to Internal Timing condition occurs when the user issues a Force command to switch to an internal timing source.

Note FRCDSWTOINT is an informational condition. It does not require troubleshooting.

2.7.95 FRCDSWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Primary Timing Source condition occurs when the user issues a Force command to switch to the primary timing source.

Note FRCDSWTOPRI is an informational condition. It does not require troubleshooting.

2.7.96 FRCDSWTOSEC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Second Timing Source condition occurs when the user issues a Force command to switch to a second timing source.

Note FRCDSWTOSEC is an informational condition. It does not require troubleshooting.

2.7.97 FRCDSWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Third Timing Source condition occurs when the user issues a Force command to switch to a third timing source.

Note FRCDSWTOTHIRD is an informational condition. It does not require troubleshooting.

2.7.98 FRNGSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE-SREF

The Free Running Synchronization Mode condition occurs when the reporting ONS 15310-CL or ONS 15310-MA is in free-run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the node has lost its designated BITS timing source. After the 24-hour holdover period expires, timing slips could begin to occur on a node relying on an internal clock.

Note If the ONS 15310-CL or ONS 15310-MA is configured to operate from its internal clock, disregard the FRNGSYNC condition.

Clear the FRNGSYNC Condition

Step 1 If the ONS 15310-CL or ONS 15310-MA is configured to operate from an external timing source, verify that the BITS timing source is valid. Refer to the "Timing" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for more information about it.

Step 2 If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as the "SYNCPRI" alarm on page 2-144 and the "SYNCSEC" alarm on page 2-145.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.99 FSTSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE-SREF

A Fast Start Synchronization Mode condition occurs when the ONS 15310-CL or ONS 15310-MA is choosing a new timing reference. The previous timing reference has failed.

The FSTSYNC condition disappears after approximately 30 seconds. If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Note FSTSYNC is an informational condition. It does not require troubleshooting.

2.7.100 FULLPASSTHR-BI

The FULLPASSTHR-BI condition is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.101 GFP-CSF

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T, CEMR, ML100T

The GFP Client Signal Fail Detected alarm is a secondary alarm raised on local GFP data ports when a remote Service-Affecting (SA) alarm causes invalid data transmission. The alarm is raised locally on CE-Series and ML-100T-8 Ethernet ports and does not indicate that a Service-Affecting (SA) failure is occurring at the local site, but that a CARLOSS, LOS, or SYNCLOSS alarm is affecting a remote data port's transmission capability. For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the GFP-CSF Alarm

Step 1 Clear the Service-Affecting (SA) alarm at the remote data port.

Step 2 If the GFP-CSF alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.7.102 GFP-EX-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: CE100T

The GFP Extension Header Mismatch alarm is raised on Fibre Channel/fiber connectivity (FICON) GFP ports when it receives frames with an extension header that is not null. The alarm occurs when a provisioning error causes all GFP frames to be dropped for 2.5 seconds. To clear this alarm, ensure that both end ports are sending a null extension header for a GFP frame.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the GFP-EX-MISMATCH Alarm

Step 1 Ensure that the vendor equipment is provisioned to send a null extension header in order to interoperate with the Fibre Channel/FICON GFP ports.

Step 2 If the GFP-EX-MISMATCH alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.7.103 GFP-LFD

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T, CEMR, ML100T

The GFP Loss of Frame Delineation alarm applies to Fibre Channel/FICON GFP ports and occurs if there is a bad SONET connection, if SONET path errors cause GFP header errors in the check sum calculated over payload length (PLI/cHEC) combination, or if the GFP source port sends an invalid PLI/cHEC combination. The loss is service affecting.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the GFP-LFD Alarm

Step 1 Look for and clear any associated SONET path errors such as LOS or AIS-L originating at the transmit node.

Step 2 If the GFP-LFD alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.7.104 GFP-UP-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T, CEMR, ML100T

The GFP User Payload Mismatch is raised against Fibre Channel/FICON ports supporting GFP. It occurs when the received frame user payload identifier (UPI) does not match the transmitted UPI and all frames are dropped. The alarm is caused by a provisioning error, such as the port media type not matching the remote port media type. For example, the local port media type could be set to Fibre Channel—1 Gbps ISL or Fibre Channel—2 Gbps ISL and the remote port media type could be set to FICON—1 Gbps ISL or FICON—2 Gbps ISL.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the GFP-UP-MISMATCH Alarm

Step 1 Ensure that the transmit port and receive port are identically provisioned for distance extension by completing the following steps:

a. Double-click the card to display the card view.

b. Click the **Provisioning > Port > Distance Extension** tabs.

c. Check the check box in the **Enable Distance Extension** column.

d. Click **Apply**.

Step 2 Ensure that both ports are set for the correct media type. For each port, complete the following steps:

a. Double-click the card to display the card view (if you are not already in card view).

b. Click the **Provisioning > Port> General** tabs.

c. Choose the correct media type (**Fibre Channel - 1Gbps ISL**, **Fibre Channel - 2 Gbps ISL**, **FICON - 1 Gbps ISL**, or **FICON - 2 Gbps ISL**) from the drop-down list.

d. Click **Apply**.

Step 3 If the GFP-UP-MISMATCH alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.7.105 HELLO

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Open Shortest Path First (OSPF) Hello alarm is raised when the two end nodes cannot bring an OSPF neighbor up to the full state. Typically, this problem is caused by an area ID mismatch, and/or an OSPF HELLO packet loss over the DCC.

Clear the HELLO Alarm

Step 1 Ensure that the area ID is correct on the missing neighbor by completing the following steps:

a. In node view, click the **Provisioning > Network > OSPF** tabs.

b. Ensure that the IP address in the Area ID column matches the other nodes.

c. If the address does not match, click the incorrect cell and correct it.

d. Click **Apply**.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.106 HIBATVG

Default Severity: Major (MJ), Service-Affecting (SA) for ONS 15310-CL

SONET Logical Object: PWR

The High Voltage Battery alarm occurs in a –48 VDC environment for the ONS 15310-CL platform when a battery lead input voltage exceeds the high power threshold. This threshold has a preset value of –55 VDC and is not user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds.

Clear the HIBATVG Alarm

Step 1 The problem is external to the ONS 15310-CL. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.107 HI-LASERBIAS

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

The Equipment High Transmit Laser Bias Current alarm is raised against OCN port laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

Laser bias typically starts at about 30 percent of the manufacturer maximum laser bias specification and increases as the laser ages. If the HI-LASERBIAS alarm threshold is set at 100 percent of the maximum, the laser usability has ended. If the threshold is set at 90 percent of the maximum, the card is still usable for several weeks or months before it needs to be replaced.

Clear the HI-LASERBIAS Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-163 for the controller card (15310-CL-CTX or CTX2500 card).

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 for commonly used traffic-switching procedures.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.108 HI-LASERTEMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

DWDM Logical Object: PPM

The Equipment High Laser Optical Transceiver Temperature alarm applies to the OC-N ports. HI-LASERTEMP occurs when the internally measured transceiver temperature exceeds the card setting by 35.6 degrees F (2 degrees C). A laser temperature change affects the transmitted wavelength.

When the card raises this alarm, the laser is automatically shut off. The "LOS (OCN)" alarm on page 2-106 is raised at the far-end node and the "DUP-IPADDR" alarm on page 2-50 is raised at the near end.

Clear the HI-LASERTEMP Alarm

Step 1 In node view, double-click the controller card (15310-CL-CTX or CTX2500 card) to display the card view.

Step 2 Click the **Performance > Optics PM** tabs.

Step 3 Verify the card laser temperature levels. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Step 4 Complete the "Soft- or Hard-Reset an Ethernet or Electrical Card in CTC" procedure on page 2-162 for the card.

Step 5 If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-163 for the card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.109 HI-RXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Equipment High Receive Power alarm is an indicator for OCN port received optical signal power. HI-RXPOWER occurs when the measured optical power of the received signal falls under the threshold. The threshold value is user-provisionable.

Clear the HI-RXPOWER Alarm

Step 1 Complete the "Clear the LO-RXPOWER Alarm" procedure on page 2-100.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.110 HITEMP

Default Severity: Critical (CR), Service-Affecting (SA) for NE; Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EQPT

SONET Logical Objects: EQPT, NE

The High Temperature alarm occurs when the temperature of the ONS 15310-CL or ONS 15310-MA is above 122 degrees F (50 degrees C).

Clear the HITEMP Alarm

Step 1 Verify that the environmental temperature of the room is not abnormally high.

Step 2 If the room temperature is not abnormal, physically ensure that nothing prevents the internal ONS 15310-CL or ONS 15310-MA fan from passing air through the ONS 15310-CL or ONS 15310-MA shelf.

Step 3 Ensure that any empty chassis slots are covered with filler cards. These aid in airflow management.

Step 4 If the alarm persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a Service-Affecting (SA) problem (1-800-553-2447) if it applies to the NE, or a Non-Service-Affecting (NSA) problem if it applies to equipment.

2.7.111 HI-TXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

The Equipment High Transmit Power alarm is an indicator on the OC-N port transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

Note For information about this alarm that applies to DWDM objects, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

Clear the HI-TXPOWER Alarm

Step 1 In node view, display the card view for the controller card (15310-CL-CTX or CTX2500 card).

Step 2 Click the **Provisioning > Optical > Optics Thresholds** tabs.

Step 3 Decrease (change toward the negative direction) the OPT-HIGH column value by 1%.

Step 4 If the card transmit power setting cannot be lowered without disrupting the signal, complete the "Physically Replace a Card" procedure on page 2-163.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 for commonly used traffic-switching procedures.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.112 HLDOVRSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE-SREF

The Holdover Synchronization Mode condition is caused by loss of the primary and second timing references in the node. Timing reference loss occurs when line coding on the timing input is different from the configuration on the node, and it often occurs during the selection of a new node reference clock. The condition clears when primary or second timing is reestablished. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15310-CL or ONS 15310-MA relying on an internal clock.

Clear the HLDOVRSYNC Alarm

Step 1 Clear additional alarms that relate to timing, such as:

- 2.7.98 FRNGSYNC, page 2-72
- 2.7.99 FSTSYNC, page 2-72
- 2.7.112 HLDOVRSYNC, page 2-79
- 2.7.135 LOF (BITS), page 2-92
- 2.7.149 LOS (BITS), page 2-101
- 2.7.170 MANSWTOINT, page 2-114
- 2.7.171 MANSWTOPRI, page 2-114
- 2.7.172 MANSWTOSEC, page 2-115
- 2.7.173 MANSWTOTHIRD, page 2-115
- 2.7.238 SWTOPRI, page 2-143
- 2.7.239 SWTOSEC, page 2-143
- 2.7.240 SWTOTHIRD, page 2-143
- 2.7.241 SYNC-FREQ, page 2-144
- 2.7.242 SYNCPRI, page 2-144
- 2.7.243 SYNCSEC, page 2-145
- 2.7.244 SYNCTHIRD, page 2-145

Step 2 Reestablish a primary and secondary timing source according to local site practice. If none exists, refer to the "Change Node Settings" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.113 I-HITEMP

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: NE

The Industrial High Temperature alarm occurs when the temperature of the ONS 15310-CL or ONS 15310-MA is above 149 degrees F (65 degrees C) or below –40 degrees F (–40 degrees C). This alarm is similar to the HITEMP alarm but is used for the industrial environment. If this alarm is used, you can customize your alarm profile to ignore the lower-temperature HITEMP alarm.

Clear the I-HITEMP Alarm

Step 1 Complete the "Clear the HITEMP Alarm" procedure on page 2-78.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.114 IMPROPRMVL

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

DWDM Logical Object: PPM

The Improper Removal equipment (IMPROPRMVL) alarm occurs under the following conditions:

- A card is removed when the card was rebooting. It is recommended that after the card completely reboots, delete the card in CTC and only then remove the card physically. When you delete the card, CTC loses connection with the node view (single-shelf mode) or shelf view (multishelf mode), and goes to network view.
- When a card is physically removed from its slot before it is deleted from CTC. It is recommended that any card be deleted in CTC before physically removing the card from the chassis.

Note CTC provides the user approximately 15 seconds to physically remove the card before it begins rebooting the card.

- A card is inserted into a slot but is not fully plugged into the backplane.
- A PPM (SFP) is provisioned but the physical module is not inserted into the port.
- Electrical issues such as short circuit or failure of DC-DC conversion.

Note For information about DWDM objects, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

Clear the IMPROPRMVL Alarm

Step 1 In node view, right-click the card reporting the IMPROPRMVL.

Step 2 Choose **Delete** from the shortcut menu.

Note CTC does not allow you to delete the reporting card if the card is in service, does have circuits mapped to it, is paired in a working protection scheme, has DCC enabled, or is used as a timing reference.

Step 3 If any ports on the card are in service, put them out of service (OOS,MT) by completing the following steps:

Caution Before placing a port out of service (OOS,MT or OOS,DSBLD), ensure that no live traffic is present.

a. In node view, double-click the controller card (15310-CL-CTX or CTX2500 card) to display the card view.
b. Click the **Provisioning > Optical > Line** tabs.
c. Click the Admin State column of any in-service (IS) ports.
d. Choose **OOS,MT** to take the ports out of service.

Step 4 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-164.

Caution Before deleting the circuit, ensure that the circuit does not carry live traffic.

Step 5 If the card is paired in a protection scheme, delete the protection group by completing the following steps:

a. Click **View > Go to Previous View** to return to node view.
b. If you are already in node view, click the **Provisioning > Protection** tabs.
c. Click the protection group of the reporting card.
d. Click **Delete**.

Step 6 If the card is provisioned for DCC, delete the DCC provisioning by completing the following steps:

a. Click the ONS 15310-CL or ONS 15310-MA **Provisioning > Comm Channels > SDCC** tabs.
b. Click the slots and ports listed in DCC terminations.
c. Click **Delete** and click **Yes** in the dialog box that appears.

Step 7 If the card is used as a timing reference, change the timing reference by completing the following steps:

a. Click the **Provisioning > Timing > General** tabs.
b. Under NE Reference, click the drop-down list for **Ref-1**.
c. Change Ref-1 from the listed source from Internal Clock.
d. Click **Apply**.

Step 8 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.115 INC-ISD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The DS-3 Idle condition indicates that the DS-3 port is receiving an idle signal from a 15310-CL-CTX, ONS 15310-MA DS1-28/DS3-EC1-3, or ONS 15310-MA DS1-84/DS3-EC1-3 DS-1 port, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting port has an OOS-MA,MT service state. It is resolved when the OOS-MA,MT state ends.

Note INC-ISD is a condition and not an alarm. It is for information only and does not require troubleshooting.

2.7.116 INCOMPATIBLE-SEND-PDIP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: SYSTEM

The Incompatible Software alarm is raised when CTC'S send PDIP provisioning differs from host node's provisioning.

Clear the INCOMPATIBLE-SEND-PDIP Alarm

Step 1 Reconfigure CTC's send PDI-P alarm capability to align with the host node settings.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.117 INCOMPATIBLE-SW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET SONET Logical Object: NE

The Incompatible Software alarm is raised when CTC cannot connect to the NE due to incompatible versions of software between CTC and the NE. The alarm is cleared by restarting CTC in order to redownload the CTC jar files from the NE.

Clear the INCOMPATIBLE-SW Alarm

Step 1 Restart the CTC application.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.118 INHSWPR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA) for ONS 15310-MA

SONET Logical Object: EQPT

The Inhibit Switch To Protect Request on Equipment condition occurs on traffic cards when the ability to switch to protect has been disabled. If the port is part of a 1+1 protection scheme, traffic remains locked onto the working system.

Clear the INHSWPR Condition

Step 1 If the condition is raised against a 1+1 port, complete the "Initiate a 1+1 Manual Switch Command" procedure on page 2-157.

Step 2 If the condition does not clear, log into the Cisco Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.119 INHSWWKG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA) for ONS 15310-MA

SONET Logical Object: EQPT

The Inhibit Switch To Working Request on Equipment condition occurs on ONS 15310-MA traffic cards when the ability to switch to working has been disabled. If the card is part of a 1+1 protection scheme, traffic remains locked onto the protect system.

Step 1 If the condition is raised against a 1+1 port, complete the "Initiate a 1+1 Manual Switch Command" procedure on page 2-157.

Step 2 If the condition does not clear, log into the Cisco Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.120 INTRUSION-PSWD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a Superuser attempts a settable number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. This condition is only shown in Superuser login sessions, not in login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a settable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if lockout is permanent.

Clear the INTRUSION-PSWD Condition

Step 1 In node view, click the **Provisioning > Security** tabs.

Step 2 Click **Clear Security Intrusion Alarm**.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.121 INVMACADR

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: BPLANE

The Equipment Failure Invalid MAC Address alarm occurs when the ONS 15310-CL or ONS 15310-MA MAC address is invalid. The MAC Address is permanently assigned to the chassis when it is manufactured. Do not attempt to troubleshoot an INVMACADR alarm. Log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.122 IOSCFGCOPY

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The IOS Configuration Copy in Progress condition occurs on ML-100T-8 Ethernet cards when a Cisco IOS startup configuration file is being uploaded or downloaded to or from an ML-100T-8 Ethernet card. (This condition is very similar to the "SFTWDOWN" condition on page 2-135 but it applies to ML-100T-8 Ethernet cards rather than to the controller card.)

The condition clears after the copy operation is complete. (If it does not complete correctly, the "NO-CONFIG" condition on page 2-119 could be raised.)

Note IOSCFGCOPY is an informational condition.

Note For more information about the Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide.*

2.7.123 ISIS-ADJ-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Open System Interconnection (OSI) Intermediate System to Intermediate-System (IS-IS) Adjacency Failure alarm is raised by an intermediate system (node routing IS Level 1 or Level 1 and 2) when no IS or end system (ES) adjacency is established on a point-to-point subnet. The Intermediate-System Adjacency Failure alarm is not supported by ES. It is also not raised by IS for disabled routers.

The alarm is typically caused by a misconfigured router manual area adjacency (MAA) address. For more information about IS-IS OSI routing and MAA configuration, refer to the "Cisco Transport Controller Operation" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*. For more information about configuring OSI, refer to the "Turn Up Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Clear the ISIS-ADJ-FAIL Alarm

Step 1 Ensure that both ends of the communications channel are using the correct Layer 2 protocol and settings (LAPD or PPP). To do this, complete the following steps:

- **a.** At the local node, in node view, click the **Provisioning > Comm Channels > SDCC** tabs.
- **b.** Click the row of the circuit. Click **Edit**.
- **c.** In the Edit SDCC termination dialog box, view and record the following selections: Layer 2 protocol (LAPD or PPP); Mode radio button selection (AITS or UITS); Role radio button selection (Network or User); MTU value; T200 value, and T203 selections.
- **d.** Click **Cancel**.
- **e.** Log into the remote node and follow the same steps, also recording the same information for this node.

Step 2 If both nodes do not use the same Layer 2 settings, you will have to delete the incorrect termination and recreate it. To delete it, click the termination and click **Delete**. To recreate it, refer to the "Turn Up Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for the procedure.

Step 3 If the nodes use PPP Layer 2, complete the "Clear the EOC Alarm" procedure on page 2-55. If the alarm does not clear, go to Step 7.

Step 4 If both nodes use the LAPD Layer 2 protocol but have different Mode settings, change the incorrect node's entry by clicking the correct setting radio button in the Edit SDCC termination dialog box and clicking **OK.**

Step 5 If the Layer 2 protocol and Mode settings are correct, ensure that one node is using the Network role and the other has the User role. If not (that is, if both have the same mode settings), correct the incorrect one by clicking the correct radio button in the Edit SDCC termination dialog box and clicking **OK**.

Step 6 If the Layer 2, Mode, and Role settings are correct, compare the MTU settings for each node. If one is incorrect, choose the correct value in the Edit SDCC dialog box and click **OK**.

Step 7 If all of the preceding settings are correct, ensure that OSI routers are enabled for the communication channels at both ends by completing the following steps:

- **a.** Click **Provisioning > OSI > Routers > Setup**.
- **b.** View the router entry under the **Status** column. If the status is Enabled, check the other end.
- **c.** If the Status is Disabled, click the router entry and click **Edit**.
- **d.** Check the **Enabled** check box and click **OK**.

Step 8 If the routers on both ends are enabled and the alarm still has not cleared, ensure that both ends of the communications channel have a common MAA by completing the following steps:

- **a.** Click the **Provisioning > OSI > Routers > Setup** tabs.
- **b.** Record the primary MAA and secondary MAAs, if configured.

Tip You can record long strings of information such as the MAA address by using the CTC export and print functions. Export it by choosing File > Export > html. Print it by choosing File > Print.

c. Log into the other node and record the primary MAA and secondary MAAs, if configured.

d. Compare this information. There should be at least one common primary or secondary MAA in order to establish an adjacency.

e. If there is no common MAA, one must be added to establish an adjacency. Refer to the "Turn Up Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures to do this.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.124 KB-PASSTHR

The KB-PASSTHR condition is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.125 LASEREOL

The LASEREOL alarm is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.126 LCAS-CRC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The Link Capacity Adjustment Scheme (LCAS) Control Word CRC Failure condition is raised against ML-100T-8 Ethernet and CE-series cards. It occurs when there is an equipment, path, or provisioning error on the virtual concatenation group (VCG) that causes consecutive 2.5 second CRC failures in the LCAS control word.

The condition can occur if an LCAS-enabled node (containing ML-100T-8 cards) transmitting to another LCAS-enabled node delivers faulty traffic due to an equipment or SONET path failure. Transmission errors would also be reflected in CV-P, ES-P, or SES-P performance-monitoring statistics. (For more information about performance-monitoring statistics, see the "Performance Monitoring" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual*.) If these errors do not exist, an equipment failure is indicated.

If LCAS is not supported on the peer node, the condition does not clear.

LCAS-CRC can also occur if the VCG source node is not LCAS-enabled, but the receiving node does have the capability enabled. Both source and destination nodes must have LCAS enabled. Otherwise, the LCAS-CRC condition persists on the VCG.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the LCAS-CRC Condition

Step 1 Look for and clear any associated equipment failures, such as the EQPT alarm, on the receive node or transmit node.

Step 2 Look for and clear any bit error rate conditions at the transmit node.

Step 3 If no equipment or SONET path errors exist, ensure that the remote node has LCAS enabled on the circuit by completing the following steps:

- **a.** In node view, click the **Circuits** tab.
- **b.** Choose the VCAT circuit and click **Edit**.
- **c.** In the Edit Circuit window, click the **General** tab.
- **d.** Verify that the Mode column says **LCAS**.

Step 4 If the column does not say LCAS, complete the "Delete a Circuit" procedure on page 2-164 and recreate it in LCAS mode using the instructions in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.127 LCAS-RX-DNU

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Receive-Side-In Do Not Use condition is raised on CE-series Ethernet and ML-100T-8 cards when the receive side of an LCAS VCG member is in the do-not use state. For a unidirectional failure, this condition is only raised at the source node.

The node reporting this condition likely reports an "RFI-P" alarm on page 2-127 and "RFI-V" alarm on page 2-127.

Note For more information about the CE-MR-6 Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the LCAS-RX-DNU Condition

Step 1 Look for any SONET failures, such as the RFI-P and RFI-V alarms, on the source node. If any are present, clear them using the relevant procedures in this chapter.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.128 LCAS-RX-FAIL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Receive-Side-In Fail condition is raised against ML-100T-8 Ethernet cards and CE-series cards with LCAS-enabled VCG or software-enabled LCAS (SW-LCAS) VCG.

LCAS VCGs treat failures unidirectionally, meaning that failures of the transmit or receive points occur independently of each other. The LCAS-RX-FAIL condition can occur on the receive side of an LCAS VCG member for the following reasons:

- SONET path failure (a unidirectional failure as seen by the receive side).
- VCAT member is set out of group at the transmit side, but is set in group at the receive side.
- VCAT member does not exist at the transmit side but does exist and is in group at the receive side.

The condition can be raised during provisioning operations on LCAS VCGs but should clear when the provisioning is completed.

Software-enabled LCAS VCGs treat failure bidirectionally, meaning that both directions of a VCG member are considered failed if either transmit or receive fails. The LCAS-RX-FAIL condition is raised on these VCG members when a member receive side fails due to a SONET path failure.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Note ONS 15310-CL ML-100T-8-Series cards are LCAS-enabled.

Clear the LCAS-RX-FAIL Condition

Step 1 Check for and clear any line or path alarms using the procedures in this chapter.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.129 LCAS-TX-ADD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Add State condition is raised against ML-100T-8 Ethernet cards and CE-series cards when the transmit side of an LCAS VCG member is in the add state. The condition clears after provisioning is completed. The condition clears after provisioning is completed. The remote likely reports a path condition such as an "AIS-P" condition on page 2-21 or an "UNEQ-P" alarm on page 2-151.

Note LCAS-TX-ADD is an informational condition and does not require troubleshooting.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide.*

2.7.130 LCAS-TX-DNU

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Do Not Use (DNU) State condition is raised on ML-100T-8 Ethernet cards and CE-series cards when the transmit side of an LCAS VCG member is in the DNU state. For a unidirectional failure, this condition is only raised at the source node. The LCAS-TX-DNU condition is raised when the cable is unplugged.

The remote node likely reports a path alarm such as AIS-P or UNEQ-P.

Note LCAS-TX-DNU is an informational condition and does not require troubleshooting.

2.7.131 LINK-KEEPALIVE

Default Severity: Critical (CR), Non-Service-Affecting (NSA)

SONET Logical Objects: ML100T

The LINK-KEEPALIVE alarm indicates that a span is not receiving a defined number of keep-alive messages on the ML-100T-8 card's IEEE 802.17b-based interface or Cisco proprietary RPR interface within allotted keep-alive timeout period. Although this alarm defaults to a Critical (CR) severity, it can be downgraded if the span is protected.

LINK-KEEPALIVE is suppressed by RPR-PASSTHR, page 129. This alarm clears when a defined number of consecutive keep-alive messages is received on the interface.

Note In the Cisco IOS CLI "show ons alarms" command display, this alarm is called KEEP-ALIVE-FAIL.

Note The GFP-UP-MISMATCH, GFP-CSF, GFP-LFD, and TPTFAIL alarms suppress the LINK-KEEPALIVE alarm even though the LINK-KEEPALIVE alarm has higher severity than the other alarms. The GFP alarms are promoted because the LINK-KEEPALIVE alarm information is contained within a GFP frame. The TPTFAIL alarm is promoted because it is a layer 1 alarm while LINK-KEEPALIVE is a layer 2 alarm.

Clear the LINK-KEEPALIVE Alarm

Step 1 Verify that no SONET or GFP circuit alarms that could impact Ethernet data traffic are present. If any are present, clear them using the relevant procedures in this chapter.

Step 2 Verify that the "DATA-CRC;" alarm on page 2-48 is not present. If it is present, complete the trouble-clearing procedure.

Step 3 Verify that the keep-alive timer on this IEEE RPR 802.17b-based station has the same value as its neighboring RPR-IEEE stations.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.132 LKOUTPR-S

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Lockout of Protection Span condition occurs when UPSR traffic is locked out of a protect span using the "Lockout of Protect" command. This condition is visible on the network view Alarms, Conditions, and History tabs after the lockout has occurred and accompanies the FE-LOCKOUTPR-SPAN condition. The port where the lockout originated is marked by an "L" on the network view detailed circuit map.

Clear the LKOUTPR-S Condition

Step 1 Complete the "Clear an External Switching Command on a Path Protection Span" procedure on page 2-161.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.133 LOA

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: VCG

The Loss of Alignment on a VCG is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when members of a VCG travel over different paths in the network (due to initial operator provisioning or to protection or restoration events) and the differential delays between the paths cannot be recovered by terminating hardware buffers.

Note This alarm occurs only if you provision circuits outside of CTC, such as by using TL1.

Clear the LOA Alarm

Step 1 In network view, click the **Circuits** tab.

Step 2 Click the alarmed VCG and then click **Edit**.

Step 3 In the Edit Circuit window, view the source and destination circuit slots, ports, and STSs.

Step 4 Identify whether the STS travels across different fibers. If it does, complete the "Delete a Circuit" procedure on page 2-164.

Step 5 Recreate the circuit using the procedure in the "Create Circuits" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.134 LOCKOUT-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: OCN, STSMON, VT-MON

The Lockout Switch Request on Facility or Equipment condition occurs when a user initiates a lockout switch request for an OC-N port in a 1+1 facility protection group. This can be accomplished by locking traffic onto the working port with the LOCK ON command (thus locking it off the protect port), or locking it off the protect port with the LOCK OUT command. In either case, the protect port will show "Lockout of Protection," and the Conditions window will show the LOCKOUT-REQ condition.

A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ Condition

Step 1 Complete the "Clear an External Switching Command on a Path Protection Span" procedure on page 2-161.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.135 LOF (BITS)

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: BITS

The Loss of Frame (LOF) BITS alarm occurs when a port on the BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15310-CL or ONS 15310-MA has lost frame delineation in the incoming data.

Clear the LOF (BITS) Alarm

Note This procedure assumes that the BITS timing reference signal is functioning properly. It also assumes the alarm is not appearing during node turn-up.

Step 1 Verify that the line type and line coding match between the BITS port and the 15310-CL-CTX or CTX2500 card by completing the following steps:

a. In node view or card view, note the slot and port reporting the alarm.

b. Find the coding and framing formats of the external BITS timing source. The formats should be in the user documentation for the external BITS timing source or on the timing source itself.

c. Click the **Provisioning > Timing > BITS Facilities** tabs.

d. Verify that the Coding setting matches the coding of the BITS timing source, either B8ZS or AMI.

e. If the coding does not match, click **Coding** and choose the appropriate coding from the drop-down list.

f. Verify that Line Type matches the line type of the BITS timing source, either ESF or SF (D4).

g. If the line type does not match, click **Line Type** and choose the appropriate framing from the drop-down list.

Note On the timing subtab, the B8ZS coding field is normally paired with ESF in the Line Type field and the AMI coding field is normally paired with SF (D4) in the Line Type field.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.136 LOF (DS1)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: DS1

The DS-1 LOF alarm indicates that the receiving ONS 15310-CL or ONS 15310-MA has lost frame delineation in an incoming DS-1 data stream. If the LOF appears on a DS-1 port, the transmitting equipment could have its line type set to a format that differs from the receiving node.

Note When the ONS 15310-MA raises an LOF (DS1) or LOS (DS1) alarm, a path protection switch will occur, but a PDI-P alarm will not be generated due to hardware limitations.

Clear the LOF (DS1) Alarm

Step 1 Verify that the line type and line coding match between the DS-1 port and the signal source by completing the following steps:

a. In CTC, note the slot and port reporting the alarm.

b. Find the coding and line type formats of the signal source for the port reporting the alarm. You might need to contact your network administrator for the format information.

c. Display the card view of the reporting DS-1 card (15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3).

d. Click the **Provisioning > DS1 > Line** tabs.

e. Verify that the line type of the reporting port matches the line type of the signal source (DS4 and DS4, unframed and unframed, or ESF and ESF). If the signal source line type does not match the reporting port, click the **Line Type** cell to reveal a drop-down list and choose the matching type.

f. Verify that the reporting Line Coding matches the signal source line coding (AMI and AMI or B8ZS and B8ZS). If the signal source line coding does not match the reporting port, click the **Line Coding** cell and choose the correct type from the drop-down list.

g. Click **Apply**.

Note On the Line tab, the B8ZS coding field is normally paired with ESF in the Line Type field. AMI coding is normally paired with SF (D4) in the Line Type field.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.137 LOF (DS3)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: DS3

The DS-3 LOF alarm indicates that the receiving 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 port has lost frame delineation in the incoming DS-3 data stream. The framing of the transmitting equipment could be set to a format that differs from the receiving system. On DS-3 ports, the alarm occurs only on when the provisionable line type format set to C bit or M13.

Clear the LOF (DS3) Alarm

Step 1 Change the line type of the non-ONS equipment attached to the reporting port to C bit by completing the following steps:

a. Double-click the 15310-CL-CTX, or DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 port to display the card view.

b. Click the **Provisioning > DS3 > Line** tabs.

c. Verify that the line type of the reporting port matches the line type of the signal source.

d. If the signal source line type does not match the reporting port, click **Line Type** and choose **C Bit** from the drop-down list.

e. Click **Apply**.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.138 LOF (EC1)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EC1

The EC1-1 LOF alarm occurs when a port on the reporting EC-1 port has an LOF condition. LOF indicates that the receiving ONS 15310-CL or ONS 15310-MA has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

Clear the LOF (EC1) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm. To verify cable continuity, follow site practices.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If cabling continuity is good, clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 3 If the alarm does not clear, see the "1.1 Network Troubleshooting Tests" section on page 1-2 to isolate the fault causing the LOF alarm.

Step 4 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a Service-Affecting (SA) problem (1-800-553-2447).

2.7.139 LOF (OCN)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: OCN, STSTRM

The LOF alarm occurs when a port on the reporting port has an LOF condition. The alarm indicates that the receiving ONS 15310-CL or ONS 15310-MA has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 ms. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

When the alarm is raised on an OC-3 or OC-12 port, it is sometimes an indication that the OC-3 or OC-12 port expects a specific line rate and the input line rate source does not match the input line rate of the optical receiver.

Clear the LOF (OCN) Alarm

Step 1 Complete the "Clear the LOF (EC1) Alarm" procedure on page 2-95.

Step 2 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a Service-Affecting (SA) problem (1-800-553-2447).

2.7.140 LOF (STSTRM)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: STSTRM

A Loss of Frame alarm for an STS circuit termination indicates that the LOF has occurred at the terminating point of the circuit (such as an OC-N port). It is similar to the "LOF (OCN)" alarm on page 2-95.

Clear the LOF (STSTRM) Alarm

Step 1 Complete the "Clear the LOF (OCN) Alarm" procedure on page 2-96.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.7.141 LOGBUFR90

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: SYSTEM

The Log Buffer Over 90 alarm indicates that the per-NE queue of incoming alarm, event, or update capacity of 5000 entries is over 90 percent full. LOGBUFR90 will clear if CTC recovers. If it does not clear, LOGBUFROVFL occurs.

Note LOGBUFR90 is an informational alarm and does not require troubleshooting.

2.7.142 LOGBUFROVFL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: SYSTEM

The Log Buffer Overflow alarm indicates that the CTC per-NE queue of incoming alarm, event, or updates, which has a capacity of 5000 entries, has overflowed. This happens only very rarely. However if it does, you must restart the CTC session. It is likely that some updates will have been missed if this alarm occurs.

Clear the LOGBUFROVFL Alarm

Step 1 Restart the CTC session.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.143 LO-LASERBIAS

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

The Equipment Low Transmit Laser Bias Current alarm is raised against OCN port or PPM laser performance. The alarm indicates that the laser has reached the minimum laser bias tolerance. If the LO-LASERBIAS alarm threshold is set at 0 percent (the default), the laser's usability has ended. If the threshold is set at 5 percent to 10 percent, the card is still usable for several weeks or months before you need to replace it.

Note For information about this alarm applies to DWDM objects, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

Clear the LO-LASERBIAS Alarm

Step 1 Complete the "Physically Replace a Card" procedure on page 2-163 for the controller card (15310-CL-CTX or CTX2500 card).

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 for commonly used traffic-switching procedures.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.144 LO-LASERTEMP

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. For more information about this alarm, refer to the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.7.145 LOM

Default Severity: Critical (CR), Service-Affecting (SA) for STSMON and STSTRM; Major (MJ) for VT-TERM

SONET Logical Objects: STSMON, STSTRM, VT-TERM

The Optical Transport Unit (OTU) Loss of Multiframe is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm applies to OCN ports when the Multi Frame Alignment Signal (MFAS) overhead field is errored for more than five frames and persists for more than 3 milliseconds.

Note Optical cards do not recognize the LOM. The system redirects the LOM alarm to the incoming side so that any optical card can display this alarm as a TERM alarm.

Clear the LOM Alarm

To clear the alarm, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.146 LOP-P

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: STSMON, STSTRM

A Loss of Pointer Path alarm indicates that the SONET path pointer in the overhead has been lost. LOP occurs when valid H1/H2 pointer bytes are missing from the overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm occurs when eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

The LOP-P alarm can occur when the received payload does not match the provisioned payload. The alarm is caused by a circuit type mismatch on the concatenation facility. For example, if an STS-1 is sent across a circuit provisioned for STS-3c, an LOP-P alarm occurs.

Clear the LOP-P Alarm

Step 1 In node view, click the **Circuits** tab and view the alarmed circuit.

Step 2 Verify the circuit size listed in the Size column. If the size is different from what is expected, such as an STS3c instead of an STS1, this raises the alarm.

Step 3 If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

For instructions to use the optical test set, consult the manufacturer.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 4 If the error is not due to an incorrectly configured test set, the error is in the provisioned CTC circuit size. Complete the "Delete a Circuit" procedure on page 2-164.

Step 5 Recreate the circuit for the correct size. For procedures, refer to the "Create Circuits" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.147 LOP-V

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: VT-MON, VT-TERM

The LOP VT alarm indicates a loss of pointer at the VT level. This alarm can occur when the received payload does not match the provisioned payload. LOP-V is caused by a circuit size mismatch on the concatenation facility.

Clear the LOP-V Alarm

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-99.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.148 LO-RXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Equipment Low Receive Power alarm is an indicator for OCN port received optical signal power. LO-RXPOWER occurs when the measured optical power of the received signal falls below the threshold value, which is user-provisionable.

Clear the LO-RXPOWER Alarm

Step 1 At the transmit end of the errored circuit, increase the transmit power level within safe limits.

Step 2 Find out whether new channels have been added to the fiber. The number of channels affects power. If channels have been added, power levels of all channels need to be adjusted.

Step 3 Find out whether gain (the amplification power) of any amplifiers has been changed. Changing amplification also causes channel power to need adjustment.

Step 4 If the alarm does not clear, remove any receive fiber attenuators or replace them with lower-resistance attenuators.

Step 5 If the alarm does not clear, inspect and clean the receive and transmit node fiber connections according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 6 If the alarm does not clear, ensure that the fiber is not broken or damaged by testing it with an optical test set. If no test set is available, use the fiber for a facility (line) loopback on a known-good port. The error reading you get is not as precise, but you generally know whether the fiber is faulty. For specific procedures to use the test set equipment, consult the manufacturer.

Step 7 If the alarm does not clear, and no faults are present on the other port(s) of the transmit or receive card, do a facility loopback on the transmit and receive ports with known-good loopback cable. Complete the "1.2.1 Perform a Facility Loopback on a Source-Node Port" procedure on page 1-4 to test the loopback.

Step 8 If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Card" procedure on page 2-163. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 9 If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.149 LOS (BITS)

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: BITS

The LOS (BITS) alarm indicates that the 15310-CL-CTX or CTX2500 card has an LOS from the BITS timing source. The LOS (BITS-N) means the BITS clock or the connection to it failed.

Clear the LOS (BITS) Alarm

Step 1 Verify the wiring connection from the BITS clock pin fields on the ONS 15310-CL or ONS 15310-MA to the timing source.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If wiring is good, verify that the BITS clock is operating properly.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.150 LOS (DS1)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: DS1

An LOS (DS1) alarm for a DS-1 port on a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card occurs when the port on the port is in service but no signal is being received. The cabling might not be correctly connected to the port, or the line could have no signal.

Note When the ONS 15310-MA raises an LOF (DS1) or LOS (DS1) alarm, a path protection switch will occur, but a PDI-P alarm will not be generated due to hardware limitations.

Clear the LOS (DS1) Alarm

Step 1 Verify that the cable is properly connected and attached to the correct port. For more information about cable connections and terminations, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 Consult site records to determine whether the port raising the alarm has been assigned.

Step 3 If the port is not currently assigned, place the port out of service using the following steps:

a. In node view, double-click the DS-1 card (15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3) to display the card view.

b. Click the **Maintenance > DS1** tabs.

c. In the Admin State column, click **OOS,DSBLD**.

d. Click **Apply**.

Step 4 If the port is assigned, verify that the correct port is in service by completing the following steps:

a. To confirm this physically, confirm that the green ACT LED is on.

b. To determine this virtually, double-click the card in CTC to display the card view and complete the following substeps:

- Click the **Provisioning > DS1> Line** tabs.
- Verify that the Admin State column lists the port as **IS**.
- If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Step 5 Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving port as possible. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 7 If a valid signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the port. To do this, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures. For more information about the cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Step 8 Repeat Steps 1 through 7 for any other port on the card that reports the LOS.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.151 LOS (DS3)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: DS3

The LOS (DS3) for a DS-3 port on a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card occurs when the port is in service but no signal is being received. The cabling might not be correctly connected to the port, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure or a fiber cut.

Note If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (DS3) Alarm

Step 1 Verify that the cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 Consult site records to determine whether the port raising the alarm has been assigned.

Step 3 If the port is not currently assigned, place the port out of service using the following steps:

a. In node view, double-click the card to display the card view.

b. Click the **Maintenance > DS3** tabs.

c. In the Admin State column, click **OOS,DSBLD**.

d. Click **Apply**.

Step 4 If the port is assigned, verify that the correct port is in service by completing the following steps:

a. To confirm this physically, confirm that the green ACT LED is on.

b. To determine this virtually, double-click the card in CTC to display the card view and complete the following substeps:

- Click the **Provisioning > DS3 > Line** tabs.
- Verify that the Admin State column lists the port as **IS**.
- If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Step 5 Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving port as possible. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected. For more information about cable connections and terminations, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 7 If a valid signal is not present and the transmitting device is operational, replace the cable connecting the transmitting device to the port. To do this, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures. For more information about the cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Step 8 Repeat Steps 1 to 7 for any other port on the card that reports the LOS.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.152 LOS (EC1)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EC1

LOS on a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card EC-1 port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (EC1) most likely means that the upstream transmitter has failed. If an EC1 LOS alarm is not accompanied by additional alarms, a cabling problem (such as an incorrect attachment, a fiber cut, or another fiber error) usually causes this alarm. The condition clears when the problem is corrected, allowing two consecutive valid frames to be received.

Note If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (EC1) Alarm

Step 1 Using site practice, verify cabling continuity to the port reporting the alarm.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If the cabling is good, verify that the correct port is in service by completing the following steps:

a. Confirm that the ACT LED is green.

b. To determine whether the port is in service, double-click the card in CTC to display the card view.

c. Click the **Provisioning > EC1 > Line** tabs.

d. Verify that the Admin State column lists the port as **IS**.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Step 3 If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving port as possible.

Step 4 If the signal is valid, ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 5 Repeat Steps 1 through 4 for any other port on the card that reports the LOS (EC1).

Step 6 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 7 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.153 LOS (FUDC)

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: FUDC

The LOS (FUDC) alarm is raised if there is a user data channel (UDC) circuit created but the port is not receiving signal input. The downstream node raises an AIS condition raised against the port transmitting the UDC. FUDC refers to the 64-kb user data channel using the F1 byte.

Clear the LOS (FUDC) Alarm

Step 1 Using site practices, verify cable continuity to the UDC port.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 Verify that there is a valid input signal using a test set. For instructions to do this, consult the test set manufacturer.

Step 3 If there is a valid signal, clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 4 If the alarm does not clear, verify that the UDC is provisioned by completing the following steps:

- **a.** At the network view, click the **Provisioning > Overhead Circuits** tabs.
- **b.** If no UDC circuit exists, create one. Refer to the "Create Circuits" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures.
- **c.** If a user data circuit exists (shown as User Data F1 under the Type column), check the source and destination ports.

Step 5 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.154 LOS (OCN)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: OCN

An LOS alarm on an OC-3 or OC-12 port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS alarm means the upstream transmitter has failed. If an OC-3 or OC-12 LOS alarm is not accompanied by additional alarms, a fiber break is usually the cause of the alarm. It clears when two consecutive valid frames are received.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (OCN) Alarm

Step 1 Using site practices, verify fiber continuity to the port.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If the cabling is good, verify that the correct port is in service by completing the following steps:

a. Confirm that the green ACT LED is on.

b. To determine whether the OC-3 or OC-12 port is in service, double-click the controller card (15310-CL-CTX or CTX2500 card) in CTC to display the card view.

c. Click the **Provisioning > Optical > Line** tabs.

d. Verify that the Admin State column lists the port as **IS**.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Step 3 If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 4 If the alarm does not clear, verify that the power level of the optical signal is within the OC-3 or OC-12 port receiver specifications. The "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* lists these specifications for each OC-N port.

Step 5 If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 6 Repeat Steps 1 to 5 for any other port on the card reporting the LOS (OC-N).

Step 7 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 8 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.155 LO-TXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

The Equipment Low Transmit Power alarm is an indicator for OCN port transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.

Clear the LO-TXPOWER Alarm

Step 1 Display the reporting card's card view.

Step 2 Click the **Provisioning > Optical > Optics Thresholds** tabs.

Step 3 Increase the TX Power Low column value by 1%.

Step 4 If the card transmit power setting cannot be increased without affecting the signal, complete the "Physically Replace a Card" procedure on page 2-163.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 for commonly used traffic-switching procedures.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 5 If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.156 LPBKCRS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Cross-Connect Loopback condition indicates that there is a software cross-connect loopback active between two OC-3 or OC-12 optical ports. A cross-connect loopback test occurs below line speed and does not affect traffic.

For more information on loopbacks, see the "1.2 Identify Points of Failure on an Electrical Circuit Path" section on page 1-3.

Note Cross-connect loopbacks occur below line speed. They do not affect traffic.

Clear the LPBKCRS Condition

Step 1 To remove the cross-connect loopback condition, double-click the 15310-CL-CTX or CTX2500 card in CTC to display the card view.

Step 2 Complete the "Clear an OC-N Port XC Loopback Circuit" procedure on page 2-165.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.157 LPBKDS3FEAC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

A Loopback Due to FEAC Command DS-3 condition occurs when a DS-3 port loopback signal is received on a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card in C-bit line type mode from the far-end node because of a FEAC command. An FEAC command is often used with loopbacks. LPBKDS3FEAC is only reported by these DS-3 ports.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKDS3FEAC Condition

Step 1 In node view, double-click the DS-3 card (15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3) to display the card view.

Step 2 Click the **Provisioning > DS3 > Line** tabs.

Step 3 Click the cell for the port in the Send Code column and click **No Code** from the drop-down list.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.158 LPBKDS3FEAC-CMD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The DS-3 Loopback Command Sent To Far End condition occurs on a near-end 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card when you send a DS-3 FEAC loopback.

Note LPBKDS3FEAC-CMD is an informational condition and does not require troubleshooting.

2.7.159 LPBKFACILITY (CE100T, CEMR)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: CE100T, CEMR

A Loopback Facility condition on a CE-Series port occurs when a software facility (line) loopback is active for a port on the card.

For information about troubleshooting optical circuits with loopbacks, refer to the "1.1 Network Troubleshooting Tests" section on page 1-2.

Clear the LPBKFACILITY (CE100T, CEMR) Condition

Step 1 Complete the "Clear an Ethernet Card Loopback Circuit" procedure on page 2-166.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.160 LPBKFACILITY (DS1, DS3)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3

A Loopback Facility condition for a DS-1 or DS-3 signal occurs when a software facility (line) loopback is active for a DS-1 or DS-3 port on a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card.

For information about troubleshooting optical circuits with loopbacks, refer to the "1.2 Identify Points of Failure on an Electrical Circuit Path" section on page 1-3. Facility loopbacks are described in the "1.1 Network Troubleshooting Tests" section on page 1-2.

Note CTC permits loopbacks to be performed on an in-service (IS) circuit. Performing a loopback is Service-Affecting (SA). If you did not perform a lock out or Force switch to protect traffic, the LPBKFACILITY condition can be accompanied by a more serious alarms such as LOS.

Note DS-3 facility (line) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted to the loopback is provided.

Clear the LPBKFACILITY (DS1, DS3) Condition

Step 1 Complete the "Clear a DS-3 or DS-1 Port Loopback Circuit" procedure on page 2-165.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.161 LPBKFACILITY (EC1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EC1

A Loopback Facility condition for an EC-1 port occurs when a software facility (line) loopback is active for a port on the reporting 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card.

For information about troubleshooting optical circuits with loopbacks, refer to the "1.1 Network Troubleshooting Tests" section on page 1-2.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKFACILITY (EC1) Condition

Step 1 Complete the "Clear an EC-1 Port Loopback" procedure on page 2-166.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.162 LPBKFACILITY (OCN)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

A Loopback Facility condition for an OC-N signal occurs when a software facility (line) loopback is active for an OC-3 or OC-12 port on the 15310-CL-CTX or CTX2500 card.

For information about troubleshooting optical circuits with loopbacks, refer to the "1.3 Identify Points of Failure on an OC-N Circuit Path" section on page 1-16. Facility loopbacks are described in the "1.1.1 Facility Loopback" section on page 1-2.

Note OC-N facility loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted to the loopback is provided.

Caution CTC permits loopbacks to be performed on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Note Before performing a facility (line) loopback on an OC-3 or OC-12 port, ensure the card contains at least two DCC paths to the node where the card is installed. A second DCC path provides a nonlooped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the ONS 15310-CL or ONS 15310-MA containing the loopback OC-3 or OC-12.

Clear the LPBKFACILITY (OCN) Condition

Step 1 Complete the "Clear an OC-N Port Facility or Terminal Loopback Circuit" procedure on page 2-165.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.163 LPKTERMINAL (CE100T, CEMR)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: CE100T, CEMR

A Loopback Terminal condition on a CE-Series port occurs when a software terminal loopback is active for a port on the card.

For information about troubleshooting optical circuits with loopbacks, refer to the "1.1 Network Troubleshooting Tests" section on page 1-2.

Clear the LPBKTERMINAL (CE100T, CEMR) Condition

Step 1 Complete the "Clear an Ethernet Card Loopback Circuit" procedure on page 2-166.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.164 LPBKTERMINAL (DS1, DS3)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3

A Loopback Terminal condition for a DS-1 or DS-3 signal occurs when a software terminal (inward) loopback is active for a DS1 or DS3 port on a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card. DS-1 and DS-3 terminal loopbacks do not typically return an AIS signal.

For information about troubleshooting optical circuits with loopbacks, refer to the "1.2 Identify Points of Failure on an Electrical Circuit Path" section on page 1-3. Facility loopbacks are described in the "1.1 Network Troubleshooting Tests" section on page 1-2.

Clear the LPBKTERMINAL (DS1, DS3) Condition

Step 1 Complete the "Clear a DS-3 or DS-1 Port Loopback Circuit" procedure on page 2-165.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.165 LPBKTERMINAL (EC1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EC1

A Loopback Terminal condition for an EC-1 port occurs when a software terminal (inward) loopback is active for an EC1 port on a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card.

For information about troubleshooting optical circuits with loopbacks, refer to the "1.1 Network Troubleshooting Tests" section on page 1-2.

Caution CTC permits loopbacks to be performed on in-service (IS) circuits. Loopbacks are Service-Affecting (SA).

Clear the LPBKTERMINAL (EC1) Condition

Step 1 Complete the "Clear an EC-1 Port Loopback" procedure on page 2-166.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.166 LPBKTERMINAL (OCN)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

A Loopback Terminal condition for an OC-N port occurs when a software terminal (inward) loopback is active for an OC-3 or OC-12 port on the 15310-CL-CTX or CTX2500 card.

Note OC-N terminal loopbacks do not typically return an AIS.

Note Performing a loopback on an in-service circuit is Service-Affecting (SA). If you did not perform a lockout or Force switch to protect traffic, the LPBKTERMINAL condition can also be accompanied by a more serious alarm such as LOS.

For information about troubleshooting electrical circuits with loopbacks, refer to the "1.2 Identify Points of Failure on an Electrical Circuit Path" section on page 1-3; for optical circuits, refer to the "1.3 Identify Points of Failure on an OC-N Circuit Path" section on page 1-16. Terminal loopbacks are described in the "1.1.2 Terminal Loopback" section on page 1-3.

Clear the LPBKTERMINAL (OCN) Condition

Step 1 Complete the "Clear an OC-N Port Facility or Terminal Loopback Circuit" procedure on page 2-165.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.167 LWBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: PWR

The Low Voltage Battery alarm occurs in a –48 VDC environment for an ONS 15310-CL when a battery lead input voltage falls below the low power threshold. This threshold has a preset value of –44 VDC and is not user-provisionable. The alarm remains raised until the voltage remains above the threshold for 120 seconds. (For information about changing this threshold, refer to the "Turn Up Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.)

Clear the LWBATVG Alarm

Step 1 The problem is external to the ONS 15310-CL or ONS 15310-MA. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.168 MAN-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, VT-MON

The Manual Switch Request condition occurs when a user initiates a Manual switch request on an OC-N port. Clearing the Manual switch clears the MAN-REQ condition. You do not need to clear the switch if you want the manual switch to remain.

Clear the MAN-REQ Condition

Step 1 Complete the "Initiate a 1+1 Manual Switch Command" procedure on page 2-157.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.169 MANRESET

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset.

Note MANRESET is an informational condition and does not require troubleshooting.

2.7.170 MANSWTOINT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE-SREF

The Manual Switch To Internal Clock condition occurs when the NE timing source is manually switched to an internal timing source.

Note MANSWTOINT is an informational condition and does not require troubleshooting.

2.7.171 MANSWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Primary Reference condition occurs when the NE timing source is manually switched to the primary timing source.

Note MANSWTOPRI is an informational condition and does not require troubleshooting.

2.7.172 MANSWTOSEC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Second Reference condition occurs when the NE timing source is manually switched to a second timing source.

Note MANSWTOSEC is an informational condition and does not require troubleshooting.

2.7.173 MANSWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to a third timing source.

Note MANSWTOTHIRD is an informational condition and does not require troubleshooting.

2.7.174 MANUAL-REQ-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Manual Switch Request on span condition occurs when a user initiates a Manual Span command to move traffic from a working span to a protect span. This condition appears on the network view Alarms, Conditions, and History tabs. The port where the MANUAL SPAN command was applied is marked with an "M" on the network view detailed circuit map.

Clear the MANUAL-REQ-SPAN Condition

Step 1 Complete the "Clear an External Switching Command on a Path Protection Span" procedure on page 2-161.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.175 MATECLK

Default Severity: Minor (MN) for ONS 15310-MA

SONET Logical Object: EQPT

The Mate Clock alarm occurs when the active CTX2500 card cannot detect the clock from the standby CTX2500 card.

Clear the MATECLK Alarm

Step 1 Complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162 for the standby CTX2500 card and wait 15 minutes.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-MA. Plug the wristband cable into either of the ESD jacks, on the far left and right faceplates in the shelf.

Step 2 If the MATECLK still persists, complete the "Physically Replace a Card" procedure on page 2-163 procedure for the standby CTX2500 card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.7.176 MEA (EQPT)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. Removing the incompatible cards clears the alarm.

Clear the MEA (EQPT) Alarm

Step 1 Physically verify the type of card that is installed in the slot reporting the MEA alarm. In node view, click the **Inventory** tab and compare it to the actual installed card.

Step 2 If you prefer the card type depicted by CTC, complete the "Physically Replace a Card" procedure on page 2-163 for the reporting card.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 3 If you prefer the card that physically occupies the slot but the card is not in service, does not have circuits mapped to it, and is not part of a protection group, place the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

Note If the card is in service, does have a circuit mapped to it, is paired in a working protection scheme, has DCC communications turned on, or is used as a timing reference, CTC does not allow you to delete the card.

Step 4 If any ports on the card are in service, place them out of service (OOS) by completing the following steps:

Caution Before placing ports out of service, ensure that live traffic is not present.

a. Double-click the reporting card to display the card view.
b. Click the **Provisioning** tab.
c. Click the **Admin State** column for any in-service ports.
d. Choose **OOS,MT** to take the ports out of service.

Step 5 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-164.

Caution Before deleting the circuit, ensure that live traffic is not present.

Step 6 If the card is paired in a protection scheme, delete the protection group by completing the following steps:

a. Click the **Provisioning > Protection** tabs.
b. Choose the protection group of the reporting card.
c. Click **Delete**.

Step 7 Right-click the card reporting the alarm.

Step 8 Choose **Delete**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.177 MEA (FAN)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: FAN

The MEA alarm is reported against the fan unit located inside the ONS 15310-CL or ONS 15310-MA if it has a fuse problem.

This alarm is not user-serviceable. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.178 MEA (PPM)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. That guide discusses all DWDM alarms.

2.7.179 MEA (SHELF)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. That guide discusses all DWDM alarms.

2.7.180 MEM-GONE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the 15310-CL-CTX or CTX2500 card. The 15310-CL-CTX or CTX2500 cards which exceed the memory capacity reboot to avoid failure of card operations.

Note The alarm does not require user intervention. The MEM-LOW alarm always preceeds the MEM-GONE alarm.

2.7.181 MEM-LOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the 15310-CL-CTX or CTX2500 card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the card is exceeded, CTC ceases to function.

Note The alarm does not require user intervention. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.182 MFGMEM

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: BPLANE, FAN, PPM

The Manufacturing Data Memory Failure alarm occurs when the electronically erasable programmable read-only memory (EEPROM) fails on a card or component, or when the 15310-CL-CTX or CTX2500 card cannot read this memory. EEPROM stores manufacturing data that a 15310-CL-CTX card uses to determine system compatibility and shelf inventory status. Unavailability of this information can cause less-significant problems.

To clear the MFGMEM alarm, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.7.183 NO-CONFIG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The No Startup Configuration condition applies to ML-100T-8 Ethernet cards and occurs when no startup configuration file has been downloaded to the 15310-CL-CTX or CTX2500 card, whether or not you preprovision the card slot. This alarm can occur during provisioning. When the startup configuration file is copied to the 15310-CL-CTX or CTX2500 card, the alarm clears.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide.*

Clear the NO-CONFIG Condition

Step 1 Create a startup configuration for the card in Cisco IOS.

General ML-100T-8 provisioning parameters are located in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*. The Guide also contains information about where to find additional IOS information.

Step 2 Upload the configuration file to the controller card by completing the following steps:

a. In node view, right-click the ML-100T-8 Ethernet card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > CTX** and navigate to the file location.

Step 3 Complete the "Soft- or Hard-Reset an Ethernet or Electrical Card in CTC" procedure on page 2-162.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.184 NON-CISCO-PPM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Object: PPM

The Non-Cisco PPM Inserted condition occurs when a PPM that is plugged into a card's port fails the security code check. The check fails when the PPM used is not a Cisco PPM.

Clear the NON-CISCO-PPM Condition

Step 1 Obtain the correct Cisco PPM and replace the existing PPM with the new one.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.185 NOT-AUTHENTICATED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: SYSTEM

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when it fails to log into a node. This alarm only displays in CTC where the login failure occurred. This alarm differs from the "INTRUSION-PSWD" alarm on page 2-84 in that INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

Note NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

2.7.186 OOU-TPT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The Out of Use Transport Failure alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) This condition is raised when a member circuit in a VCAT is unused. It occurs in conjunction with the "VCG-DEG" alarm on page 2-154.

Clear the OOT-TPT Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-154. Clearing that condition clears this condition as well.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.187 OPEN-SLOT

Default Severity: Not Alarmed (NA)

SONET Logical Object: EQPT

The Open Slot condition indicates that there is an open slot in the system shelf. Slot covers assist with airflow and cooling.

Clear the OPEN-SLOT Condition

Step 1 To install a slot cover and clear this condition, refer to the procedures located in the "Install Hardware" chapter of the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.188 PDI-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

A PDI-P is a set of application-specific codes indicating a signal label mismatch failure (SLMF) in the ONS 15310-CL or ONS 15310-MA STS path overhead. The condition indicates to downstream equipment that a defect is present in one or more of the directly mapped payloads contained in that STS synchronous payload envelope (SPE). For example, the mismatch could occur in the overhead to the path selector in a downstream node configured as part of a UPSR. The PDI-P codes appear in the STS Signal Label (C2 byte).

An SLMF often occurs when the payload does not match what the signal label is reporting. The "AIS" condition on page 2-20 often accompanies a PDI-P condition. If the PDI-P is the only condition reported with the AIS, clearing PDI-P clears the AIS. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on an OC-3 or OC-12 port supporting an ONS 15310-CL or ONS 15310-MA Ethernet card circuit could result from the end-to-end Ethernet link integrity feature of the Ethernet card. If the link integrity is the cause of the path defect, it is typically accompanied by the "CARLOSS (EQPT)" alarm on page 2-39 reported against one or both Ethernet ports terminating the circuit. If this is the case, clear the TPTFAIL and CARLOSS alarms to resolve the PDI-P condition.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the PDI-P Condition

Step 1 Verify that all circuits terminating in the reporting card are in an active state by completing the following steps:

a. Click the **Circuits** tab.

b. Verify that the **Status** column lists the port as active.

c. If the Status column lists the port as incomplete, wait 10 minutes for the ONS 15310-CL or ONS 15310-MA to initialize fully. If the incomplete state does not change after full initialization, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a Service-Affecting (SA) problem (1-800-553-2447).

Step 2 After determining that the port is active, ensure that the signal source to the card reporting the alarm is working.

Step 3 If traffic is affected, complete the "Delete a Circuit" procedure on page 2-164.

Caution Deleting a circuit can affect existing traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the "Create Circuits" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide* for procedures.

Step 5 If the circuit deletion and re-creation does not clear the condition, verify that there is no problem with the far-end OC-3 or OC-12 port providing STS payload to the reporting card.

Step 6 If the condition does not clear, confirm that the cross-connect between the OC-3 or OC-12 port and the reporting port is good.

Step 7 If the condition does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 8 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.189 PLM-P

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: STSMON, STSTRM

A Payload Label Mismatch Path alarm indicates that signal does not match its label. The condition is indicated by an invalid C2 byte value in the SONET path overhead.

This alarm can occur on a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card when it expects a DS-1 signal but receives a DS-3 signal. The DS-3 signal C2 byte value is 4, so this causes a label mismatch and a PLM-P alarm.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the PLM-P Alarm

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-122.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.190 PLM-V

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: VT-TERM, VT-MON

A Payload Label Mismatch VT Layer alarm raises when the content of the V5 byte in the SONET overhead is inconsistent or invalid. PLM-V occurs when ONS 15310-CLs or ONS 15310-MAs interoperate with equipment that performs bit-synchronous mapping for DS-1 signal. The node uses asynchronous mapping.

Clear the PLM-V Alarm

Step 1 Verify that your signal source matches the signal allowed by the traffic card. For example, the alarm will occur if your signal source uses VT6 or VT9 mapping, because this is not supported by a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card.

Step 2 If the signal source matches the card, verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.191 PORT-MISMATCH

The PORT-MISMATCH alarm is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.192 PRC-DUPID

The PRC-DUPID alarm is not used in the ONS 15310 platforms in this release. It is reserved for development.

2.7.193 PROTNA

Default Severity: Minor (MN) for ONS 15310-MA

SONET Logical Object: EQPT

The Protection Unit Not Available alarm is caused by an OOS protection card when a CTX2500 card that has been provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

Clear the PROTNA Alarm

Step 1 If the PROTNA alarm occurs and does not clear, and if it is raised against a controller or cross-connect card, ensure that there is a redundant CTX2500 card installed and provisioned in the chassis.

Step 2 If the alarm is raised against a line card, verify that the ports have been taken out of service (OOS,MT):

- **a.** In CTC, double-click the reporting card to open the card view (if the card is not an cross-connect card).
- **b.** Click the Provisioning tab.
- **c.** Click the **Admin State** column of any in-service (IS) ports.
- **d.** Choose **OOS,MT** to take the ports out of service.

Step 3 Complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162 for the reporting card. For the LED behavior, see the "2.9.2 Typical Card LED Activity During Reset" section on page 2-156.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" procedure on page 2-163 for the reporting card.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.194 PROV-MISMATCH

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. That guide discusses all DWDM alarms.

2.7.195 PWR-FAIL-A

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical line card or the controller card.

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.** Statement 43

Clear the PWR-FAIL-A Alarm

Step 1 If a single port has reported the alarm, take the following actions depending on the reporting entity:

- If the reporting port is an active traffic line port in a 1+1 protection group or part of a UPSR, ensure that an APS traffic switch has occurred to move traffic to the protect port.

  Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 for commonly used traffic-switching procedures.

- If the alarm is reported against a 15310-CL-CTX or CTX2500 card, complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162.

Step 2 If the alarm does not clear, reseat the power cable connection to the connector. For more information about power connections, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 3 If the alarm does not clear, physically replace the power cable connection to the connector.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.196 PWR-FAIL-B

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical line card or the controller card.

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.** Statement 43

Clear the PWR-FAIL-B Alarm

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-125.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.197 RAI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3

The Remote Alarm Indication (RAI) condition signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other. RAI on a DS-3 port indicates that the far-end node is receiving a DS-3 AIS.

Clear the RAI Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-21.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.198 RFI-L

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: EC1, OCN

A Remote Fault Indication (RFI) Line condition occurs when the ONS 15310-CL or ONS 15310-MA detects an RFI in OC-3 or OC-12 port SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Clear the RFI-L Condition

Step 1 Log into the node at the far-end of the reporting ONS 15310-CL or ONS 15310-MA.

Step 2 Identify and clear any alarms, particularly the "LOS (OCN)" alarm on page 2-106.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.199 RFI-P

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

An RFI Path condition occurs when the ONS 15310-CL or ONS 15310-MA detects an RFI in the an STS-1 signal SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P condition in the reporting node. RFI-P occurs in the terminating node in that path segment.

Clear the RFI-P Condition

Step 1 Verify that the ports are enabled and in service (IS) on the reporting ONS 15310-CL or ONS 15310-MA by completing the following steps:

a. Confirm that the green ACT LED is on.

b. To determine whether the OC-3 or OC-12 port is in service, double-click the 15310-CL-CTX or CTX2500 card in CTC to display the card view.

c. Click the **Provisioning > Optical > Line** tabs.

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS, click the column and choose **IS**. Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Step 2 To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.

Step 3 Clear alarms in the node with the failure, especially the "UNEQ-P" alarm on page 2-151.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.200 RFI-V

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: VT-MON, VT-TERM

An RFI VT Layer condition occurs when the ONS 15310-CL or ONS 15310-MA detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V condition in the reporting node. RFI-V indicates that an upstream failure has occurred at the VT layer.

Clear the RFI-V Condition

Step 1 Verify that the fiber connectors are securely fastened and connected to the correct slot. For more information, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If connectors are correctly connected, verify that the port is active and in service (IS-NR) by completing the following steps:

a. Confirm that the green ACT LED is on.

b. Double-click the 15310-CL-CTX or CTX2500 card in CTC to display the card view.

c. Click the **Provisioning > Optical > Line** tabs.

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Step 3 If the ports are active and in service, use an optical test set to verify that the signal source does not have errors. For specific procedures to use the test set equipment, consult the manufacturer.

Step 4 If the signal is valid, log into the node at the far-end of the reporting ONS 15310-CL or ONS 15310-MA.

Step 5 Clear alarms in the far-end node, especially the "UNEQ-P" alarm on page 2-151 or the "UNEQ-V" alarm on page 2-153.

Step 6 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.201 ROLL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM, VT-MON, VT-TERM

The ROLL condition indicates that circuits are being rolled. This is typically done to move traffic for a maintenance operation or to perform bandwidth grooming. The condition indicates that a good signal has been received on the roll destination leg, but the roll origination leg has not yet been dropped. The condition clears when the roll origination leg is dropped.

Note ROLL is an informational condition and does not require troubleshooting.

2.7.202 ROLL-PEND

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA) for STSMON, VT-MON, VT-TERM; Not Reported (NR), Non-Service-Affecting (NSA) for STSTRM

SONET Logical Objects: STSMON, VT-MON, VT-TERM

ROLL-PEND indicates that a roll process has been started, but a good signal has not been received yet by the roll destination leg. This condition can be raised individually by each path in a bulk circuit roll.

The condition clears when a good signal has been received on the roll destination leg.

Note ROLL-PEND is an informational condition and does not require troubleshooting.

2.7.203 ROUTE-OVERFLOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: NE

DWDM Logical Object: NE regardless of MSTP or MSPP

The ROUTE-OVERFLOW indicates the condition when the OSPF routing table exceeds 700 routes. The symptoms for this condition are loss of visibility to a node or network, inability to access a node using CTC, CTM, Telnet, Ping, and so on.

Clear the ROUTE-OVERFLOW Condition

Step 1 Reconfigure the OSPF network to less than 700 routes.

2.7.204 RPR-PASSTHR

The RPR-PASSTHR condition is not used in the Cisco ONS 15310 platforms in this release. It is reserved for development.

2.7.205 RPRW

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: CE100T, ML100T

The Resilient Packet Ring (RPR) Wrapped condition applies to the CE-100T-8 and ML-100T-8 card. It occurs when the RPR protocol initiates a ring wrap due to a fiber cut, node failure, node restoration, new node insertion, or other traffic problem. When the wrap occurs, traffic is redirected to the original destination by sending it in the opposite direction around the ring after a link state change or after receiving any SONET path-level alarms.

Clear the RPRW Condition

Step 1 Look for and clear any service-affecting SONET path-level alarms on the affected circuit, such as the "LOP-P" alarm on page 2-98, "PLM-P" alarm on page 2-122, or the "TIM-P" alarm on page 2-148. Clearing this alarm can also clear RPRW.

Step 2 If the condition does not clear, look for and clear any service alarms for the Ethernet card itself, such as the "CARLOSS (CE100T, CEMR)" alarm on page 2-37 or the "TPTFAIL" alarm on page 2-149.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.206 RUNCFG-SAVENEED

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Run Configuration Save Needed condition occurs when you change the running configuration file for ML-100T-8 card. It is a reminder that you must save the change to the startup configuration file for it to be permanent.

The condition clears after you save the running configuration to the startup configuration, such as by entering the following command at the CLI:

```
copy run start
```

at the privileged EXEC mode of the Cisco IOS CLI. If you do not save the change, the change is lost after the card reboots. If the command "copy run start" is executed in configuration mode and not privileged EXEC mode, the running configuration will be saved, but the alarm will not clear.

2.7.207 SD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3

A Signal Degrade condition for a DS-1 or DS-3 signal on a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 card occurs when the quality of an electrical signal has exceeded the BER signal degrade threshold. Signal degrade is defined by Telcordia as a soft failure condition. SD and signal fail (SF) both monitor the incoming BER and are similar conditions, but SD is triggered at a lower bit error rate than SF.

The BER threshold is user-provisionable and has a range for SD from 1E–9 dBm to 1E–5 dBm.

SD can be reported on electrical ports that are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AIS); or OOS-MA,MT, but not in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. The BER count increase associated with this alarm does not take an IS-NR port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem (including a faulty fiber connection), a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated 15310-CL-CTX card resets that in turn can cause switching on the lines or paths.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note Some levels of BER errors (such as 1E–9 dBm) take a long period of time to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 1E–9 dBm rate, the SD alarm needs at least one and one-half hours to raise and then another period at least as long to clear.

Note The recommended test set for use on all SONET ONS electrical ports is the Omniber 718.

Clear the SD (DS1, DS3) Condition

Step 1 Complete the "Clear a DS-3 or DS-1 Port Loopback Circuit" procedure on page 2-165.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 Ensure that the fiber connector for the port is completely plugged in. For more information about cable connections, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 3 If the BER threshold is correct and at the expected level, use a test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

Step 4 If the power level is good, verify that receive levels are within the acceptable range. The correct specifications are listed in the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 5 If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 6 If the condition does not clear, verify that single-mode fiber is used.

Step 7 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 8 Clean the fiber connectors at both ends for a signal degrade according to site practice. If no practice exists, use the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 9 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement.

Step 10 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.208 SD-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EC1, OCN

An SD Line condition applies to the line level of the SONET signal and travels on the B2 byte of the SONET overhead for a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 EC1 signal, or a for a 15310-CL-CTX or CTX2500 card. An SD-L condition on an Ethernet card or OC-3 port does not cause a protection switch. If the condition is reported on a port that has also undergone a protection switch, the SD BER count continues to accumulate. The condition is superseded by higher-priority alarms such as 2.7.139 LOF (OCN) or 2.7.154 LOS (OCN).

Clear the SD-L Condition

Step 1 Complete the "Clear an OC-N Port Facility or Terminal Loopback Circuit" procedure on page 2-165.

Step 2 Ensure that the fiber connector for the port is completely plugged in. For more information about fiber connections, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 3 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

Step 4 If the optical power level is good, verify that optical receive levels are within the acceptable range. The correct specifications are listed in the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 5 If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 6 If the condition does not clear, verify that single-mode fiber is used.

Step 7 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 8 Clean the fiber connectors at both ends for a signal degrade according to site practice.

Step 9 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement.

Step 10 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.209 SD-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

An SD Path condition applies to the path (STS) layer of the SONET overhead. A path or ST-level SD alarm travels on the B3 byte of the SONET overhead.

For UPSR-protected circuits, the BER threshold is user-provisionable and has a range for SD from 1E–9 dBm to 1E–5 dBm. For 1+1 and unprotected circuits, the BER threshold value is not user-provisionable and the error rate is hard-coded to 1E–6 dBm. An SD-P condition causes a switch from the working port to the protect port at the path (STS) level.

The BER increase that causes the condition is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

SD causes the port to switch from working to protect. The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered it.

Clear the SD-P Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-132.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.210 SD-V

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: VT-MON, VT-TERM

An SD-V condition is similar to the "SD" condition on page 2-130, but it applies to the VT layer of the SONET overhead.

For UPSR protected circuits, the BER threshold is user-provisionable and has a range for SD from 1E–9 dBm to 1E–5 dBm. An SD-V condition does not cause a switch from the working port to the protect port at the path (STS) level.

The BER increase that causes the alarm is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

SD causes the port to switch from working to protect. The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered it.

Clear the SD-V Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-131.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.211 SF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3

A Signal Fail condition occurs when the quality of the signal has exceeded the BER signal failure threshold. Signal failure is defined by Telcordia as a "hard failure" condition. The SD and SF conditions both monitor the incoming BER error rate and are similar conditions, but SF is triggered at a higher BER than SD.

The BER threshold is user-provisionable and has a range for SF from 1E–5 to 1E–3.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the SF (DS1, DS3) Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-131.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.212 SF-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EC1, OCN

An SF Line condition applies to the line layer B2 overhead byte of the SONET signal. It can trigger a protection switch. The SF-L condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The condition is superseded by higher-priority alarms such as 2.7.139 LOF (OCN) or 2.7.154 LOS (OCN).

Clear the SF-L Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-132.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.213 SF-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

An SF Path condition is similar to an "SF-L" condition on page 2-134, but it applies to the path (STS) layer B3 byte of the SONET overhead. It can trigger a protection switch.

The SF-P condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Clear the SF-P Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-132.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.214 SFTWDOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

A Software Download in Progress alarm occurs when the 15310-CL-CTX or CTX2500 card is downloading or transferring software.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Note SFTWDOWN is an informational alarm.

2.7.215 SF-V

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: VT-MON, VT-TERM

An SF-V condition is similar to the "SF" condition on page 2-134, but it applies to the VT layer of the SONET overhead.

Clear the SF-V Condition

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-132.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.216 SHELF-COMM-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. That guide discusses all DWDM alarms.

2.7.217 SNTP-HOST

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an ONS 15310-CL or ONS 15310-MA serving as an IP proxy for the other nodes in the ring is not forwarding SNTP information to the other nodes in the network. The forwarding failure can result from two causes: either the IP network attached to the ONS proxy node is experiencing problems, or the ONS proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

Step 1 Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet by completing the procedure in the "1.9.8 Verify Microsoft Windows PC Connection to the Node (Ping)" section on page 1-68.

Step 2 If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems which could affect the SNTP server/router connecting to the proxy ONS system.

Step 3 If no network problems exist, ensure that the ONS 15310-CL or ONS 15310-MA proxy is provisioned correctly by completing the following steps:

- **a.** In node view for the node serving as the proxy, click the **Provisioning > General** tabs.
- **b.** Ensure that the Use NTP/SNTP Server check box is checked.
- **c.** If the Use NTP/SNTP Server check box is not checked, click it.
- **d.** Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.

Step 4 If proxy is correctly provisioned, refer to the "Cisco Transport Controller Operation" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Reference Manual* for more information on SNTP Host for general information about working with SNTP. Refer to the "Turn Up Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.218 SQM

Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Major (MJ), Service-Affecting (SA) for VT-TERM

SONET Logical Objects: STSTRM, VT-TERM

The Sequence Mismatch alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when the expected sequence numbers of VCAT members do not match the received sequence numbers.

Clear the SQM Alarm

Step 1 For the errored circuit, complete the "Delete a Circuit" procedure on page 2-164.

Step 2 Recreate the circuit using the procedure in the "Create Circuits" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.219 SSM-DUS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, OCN

The Synchronization Status (SSM) Message Quality Changed to Do-Not-Use (DUS) condition occurs when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. The DUS signal can also be sent for line maintenance testing.

Note SSM-DUS is an informational condition. It does not require troubleshooting.

2.7.220 SSM-FAIL

Single Failure Default Severity: Minor (MN), Non-Service-Affecting (NSA); Double Failure Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: BITS, DS1, OCN

The SSM Failed alarm occurs when the synchronization status messaging received by the ONS 15310-CL or ONS 15310-MA fails. The problem is external to the system. This alarm indicates that although the system is set up to receive SSM, the timing source is not delivering valid SSM messages.

Clear the SSM-FAIL Alarm

Step 1 Verify that SSM is enabled on the external timing source.

Step 2 If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM. For specific procedures to use the test set equipment, consult the manufacturer.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.221 SSM-LNC

The SSM-LNC condition is not used in this platform in this release. It is reserved for development.

2.7.222 SSM-OFF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, OCN

The SSM Off condition applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The condition is raised when the ONS system is set up to receive SSM, but the timing source is not delivering SSM messages.

Clear the SSM-OFF Condition

Step 1 Complete the "Clear the SSM-FAIL Alarm" procedure on page 2-138.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.223 SSM-PRC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SDH Logical Objects: BITS, DS1, NE-SREF, OCN

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level is changed to Stratum 1 Traceable.

Note SSM-PRC is an informational condition. It does not require troubleshooting.

2.7.224 SSM-PRS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, NE-SREF, OCN

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level is changed to Stratum 1 Traceable.

Note SSM-PRS is an informational condition. It does not require troubleshooting.

2.7.225 SSM-RES

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, NE-SREF, OCN

The SSM Reserved (RES) For Network Synchronization Use condition occurs when the synchronization message quality level is changed to RES.

Note SSM-RES is an informational condition. It does not require troubleshooting.

2.7.226 SSM-SDH-TN

The SSM-SDH-TN condition is not used in this platform in this release. It is reserved for development.

2.7.227 SSM-SETS

The SSM-SETS condition is not used in this platform in this release. It is reserved for development.

2.7.228 SSM-SMC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, NE-SREF, OCN

The SSM SONET Minimum Clock (SMC) Traceable condition occurs when the synchronization message quality level changes to SMC. The login node does not use the clock because the node cannot use any reference beneath its internal level, which is ST3.

Note SSM-SMC is an informational condition. It does not require troubleshooting.

2.7.229 SSM-ST2

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, NE-SREF, OCN

The SSM Stratum 2 (ST2) Traceable condition occurs when the synchronization message quality level is changed to ST2.

Note SSM-ST2 is an informational condition. It does not require troubleshooting.

2.7.230 SSM-ST3

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, NE-SREF, OCN

The SSM Stratum 3 (ST3) Traceable condition occurs when the synchronization message quality level is changed to ST3.

Note SSM-ST3 is an informational condition. It does not require troubleshooting.

2.7.231 SSM-ST3E

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, NE-SREF, OCN

The SSM Stratum 3E (ST3E) Traceable condition indicates that the synchronization message quality level is changed to ST3E from a lower level of synchronization. SSM-ST3E is a Generation 2 SSM and is not used for Generation 1.

Note SSM-ST3E is an informational condition. It does not require troubleshooting.

2.7.232 SSM-ST4

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, NE-SREF, OCN

The SSM Stratum 4 (ST4) Traceable condition occurs when the synchronization message quality level is lowered to ST4. The message quality is not used because it is below ST3.

Note SSM-ST4 is an informational condition. It does not require troubleshooting.

2.7.233 SSM-STU

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, NE-SREF, OCN

The SSM Synchronization Traceability Unknown (STU) condition occurs when the reporting node is timed to a reference that does not support SSM, but the ONS 15310-CL or ONS 15310-MA has SSM support enabled. SSM-STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the system.

Clear the SSM-STU Condition

Step 1 In node view, click the **Provisioning > Timing > BITS Facilities** tabs.

Step 2 If the **Sync. Messaging Enabled** check box for the BITS source is checked, uncheck the box.

Step 3 If the **Sync. Messaging Enabled** check box for the BITS source is not checked, check the box.

Step 4 Click **Apply**.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.234 SSM-TNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, NE-SREF, OCN

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is changed to TNC.

Note SSM-TNC is an informational condition. It does not require troubleshooting.

2.7.235 SW-MISMATCH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Software Mismatch condition occurs during software upgrade when there is a mismatch between software versions. The card connecting to the CTX-2500 card is running an older version than the CTX-2500 card is.

Clear the SW-MISMATCH Condition

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, position the cursor over the optical or electrical traffic card slot reporting the alarm.

Step 3 Right-click the card. Choose **Reset Card** from the shortcut menu.

Step 4 Click **Yes** in the Resetting Card dialog box.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.236 SWMTXMOD-PROT

Default Severity: Critical (CR), Service-Affecting (SA) for ONS 15310-MA

SONET Logical Object: EQPT

The Switching Matrix Module Failure on Protect Slot alarm is raised by the Slot 4 CTX2500 card if this card is active (ACT). SWMTXMOD-PROT occurs when a logic component internal to the is out of frame (OOF) with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

Clear the SWMTXMOD-PROT Alarm

Step 1 Complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162 procedure for the Slot 4 card. For the LED behavior, see the "2.9.2 Typical Card LED Activity During Reset" section on page 2-156.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) a Card" section on page 2-163 procedure for the Slot 4 controller card.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.7.237 SWMTXMOD-WORK

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Switching Matrix Module Failure on Working Slot alarm is raised by the 15310-CL-CTX or CTX2500 card when a logic component internal to the card's cross connect is OOF with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

Clear the SWMTXMOD-WORK Alarm

Step 1 Complete the "Soft- or Hard-Reset an Ethernet or Electrical Card in CTC" procedure on page 2-162 for the controller card. For the LED behavior, see the "2.9.2 Typical Card LED Activity During Reset" section on page 2-156.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.238 SWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Primary Reference condition occurs when the ONS 15310-CL or ONS 15310-MA switches to the primary timing source (reference 1). The system uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Note SWTOPRI is an informational condition. It does not require troubleshooting.

2.7.239 SWTOSEC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Secondary Reference condition occurs when the ONS 15310-CL or ONS 15310-MA has switched to a secondary timing source (reference 2).

Clear the SWTOSEC Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-144.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.240 SWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Third Reference condition occurs when the ONS 15310-CL or ONS 15310-MA has switched to a third timing source (reference 3).

Clear the SWTOTHIRD Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-144 or the "SYNCSEC" alarm on page 2-145.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.241 SYNC-FREQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, OCN

The Synchronization Reference Frequency Out Of Bounds condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

Clear the SYNC-FREQ Condition

Step 1 Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency. For specific procedures to use the test set equipment, consult the manufacturer. For BITS, the proper timing frequency range is approximately –15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately –16 PPM to 16 PPM.

Step 2 If the SYNC-FREQ condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.242 SYNCPRI

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF; Major (MJ), Service-Affecting (SA) for NE-SREF

SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the ONS 15310-CL or ONS 15310-MA loses the primary timing source (reference 1). The system uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the system should switch to its secondary timing source (reference 2). Switching to a secondary timing source also triggers the "SWTOSEC" alarm on page 2-143.

Clear the SYNCPRI Alarm

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Verify the current configuration for REF-1 of the NE Reference.

Step 3 If the primary timing reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-101.

Step 4 If the primary reference clock is an incoming port on the ONS 15310-CL or ONS 15310-MA, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-106.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.243 SYNCSEC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15310-CL or ONS 15310-MA loses a secondary timing source (reference 2). If SYNCSEC occurs, the system should switch to a third timing source (reference 3) to obtain valid timing. Switching to a third timing source also triggers the "SWTOTHIRD" alarm on page 2-143.

Clear the SYNCSEC Alarm

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Verify the current configuration of REF-2 for the NE Reference.

Step 3 If the second reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-101.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the secondary timing source is an incoming port on the ONS 15310-CL or ONS 15310-MA, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-106.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.244 SYNCTHIRD

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference alarm occurs when the ONS 15310-CL or ONS 15310-MA loses the third timing source (reference 3). If SYNCTHIRD occurs and the system uses an internal reference for source three, the 15310-CL-CTX card or CTX2500 card could have failed. The system often reports either the "FRNGSYNC" condition on page 2-72 or the "HLDOVRSYNC" condition on page 2-79 after a SYNCTHIRD alarm.

Clear the SYNCTHIRD Alarm

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Verify that the current configuration of REF-3 for the NE Reference. For more information about references, refer to the "Turn Up Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 3 If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-101.

Step 4 If the third timing source is an incoming port on the ONS 15310-CL or ONS 15310-MA, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-106.

Step 5 If the third timing source uses internal timing, complete the "Soft- or Hard-Reset a Controller Card" procedure on page 2-162.

Step 6 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447).

2.7.245 SYSBOOT

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: NE

The System Reboot alarm indicates that new software is booting on the 15310-CL-CTX or CTX2500 card. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

Note SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

2.7.246 TIM

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: OCN

The Section TIM alarm occurs when the expected J0 section trace string does not match the received section trace string. This occurs because the data being received is not correct or the receiving port could not connect to the correct transmitter port.

If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed due to a fibering misconnection, a TL1 routing change, or to someone entering an incorrect value in the Current Transmit String field.

TIM occurs on a port that has previously been operating without alarms if someone switches optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the "LOF (OCN)" alarm on page 2-95 or the "UNEQ-P" alarm on page 2-151. If these alarms accompany a TIM alarm, reattach or replace the original cables/fibers to clear the alarms. If a Transmit or Expected String was changed, restore the original string.

Clear the TIM Alarm

Step 1 Ensure that the physical fibers are correctly configured and attached. To do this, consult site documents. For more information about cabling the ONS 15310-CL or ONS 15310-MA, refer to the "Install Hardware" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If the alarm does not clear, you can compare the J0 expected and transmitted strings and, if necessary, change them by completing the following steps:

a. Log into the circuit source node and click the **Circuits** tab.

b. Select the circuit reporting the condition, then click **Edit**.

c. In the Edit Circuit window, check the **Show Detailed Circuit Map** check box and click **Apply**.

d. On the detailed circuit map, right-click the source circuit port and choose **Edit J0 Path Trace (port)** from the shortcut menu.

e. Compare the Current Transmit String and the Current Expected String entries in the Edit J0 Path Trace dialog box.

f. If the strings differ, correct the Transmit or Expected strings and click **Apply**.

g. Click **Close**.

Step 3 If the alarm does not clear, ensure that the signal has not been incorrectly routed. (Although the ONS 15310-CL or ONS 15310-MA routes circuits automatically, the circuit route could have been changed using TL1.) If necessary, manually correct the routing using TL1. For instructions, refer to the *Cisco ONS SONET TL1 Reference Guide* and the *Cisco SONET TL1 Command Guide*.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem if necessary.

2.7.247 TIM-MON

Default Severity: Minor (MN)

SONET Logical Object: OCN

The TIM Section Monitor TIM alarm applies to TXP and MXP cards. For information about this alarm, refer to the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.7.248 TIM-P

Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Minor (MN), Non-Service-Affecting (NSA) for STSMON

SONET Logical Objects: STSMON, STSTRM

The TIM Path alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to Manual or Auto for the TIM-P alarm to occur.

In manual mode at the Path Trace window, the user types the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-P alarm. In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either instance.

Clear the TIM-P Alarm

Step 1 Complete the "Clear the TIM Alarm" procedure on page 2-147. (The option will say "Edit J1 Path Trace" rather than "Edit J0 Path Trace.")

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447). If the alarm applies to the STSTRM object, it is Service-Affecting (SA).

2.7.249 TIM-S

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: EC1, OCN

The TIM for Section Overhead alarm occurs when there is a mismatch between the expected and received J0 section overhead strings in either Manual or Auto mode.

In manual mode at a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 Section Trace window, the user enters the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-S alarm.

In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either problem.

TIM-S also occurs on a port that has previously been operating without alarms if someone switches the cables or optical fibers that connect the ports. If enabled on the port, the "AIS-L" condition on page 2-21 can be raised downstream and the "RFI-L" condition on page 2-126 can be raised upstream.

Clear the TIM-S Alarm

Step 1 Double-click the 15310-CL-CTX or CTX2500 card to display the card view.

Step 2 For the 15310-CL-CTX, click the **Maintenance > EC1 > Path Trace** tabs; for the CTX2500 card, click the **Maintenance > Optical > Path Trace** tabs.

Step 3 In the Expected String column, enter the correct string information.

Step 4 Click **Apply**.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447). If the alarm applies to the STSTRM object, it is Service-Affecting (SA).

2.7.250 TIM-V

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: VT-TERM, VT-MON

The VT Path TIM alarm is raised on VT terminations when the J2 path trace is enabled and is mismatched with the expected trace string.

Clear the TIM-V Alarm

Step 1 Complete the "Clear the TIM Alarm" procedure on page 2-147.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a service-affecting problem.

2.7.251 TPTFAIL

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T, CEMR, ML100T

The Transport (TPT) Layer Failure alarm for the CE-Series or ML-100T-8 card indicates a break in the end-to-end Ethernet link integrity feature of these cards. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the TPTFAIL Alarm

Step 1 Clear any alarms being reported by the OC-N port on the CE-Series or ML-100T-8 circuit.

Step 2 If no alarms are reported by the OC-N port, or if the "PDI-P" condition on page 2-121 is reported, the problem could be on the far-end G-Series Ethernet port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.252 TX-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1

The Transmit (TX) Direction AIS condition is raised by the ONS 15310-MA backplane when it receives a far-end DS-1 LOS.

Clear the TX-AIS Condition

Step 1 Determine whether there are alarms on the downstream nodes and equipment, especially the "LOS (OCN)" alarm on page 2-106, or OOS ports.

Step 2 Clear the downstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.253 TX-LOF

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1

The Transmit Direction LOF condition is transmitted by the ONS 15310-MA backplane when it receives a DS-1 TX-LOF.

This alarm is raised only at the transmit (egress) side.

Clear the TX-LOF Condition

Step 1 Complete the "Clear the LOF (DS1) Alarm" procedure on page 2-94.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.254 TX-RAI

Default Severity: Not Alarmed (NA)

SONET Logical Objects: DS1, DS3

The Transmit Direction RAI condition is transmitted by the backplane when it receives a 15310-CL-CTX, DS1-28/DS3-EC1-3, or DS1-84/DS3-EC1-3 DS-1 TX-AIS. This alarm is raised only at the transmit side, but RAI is raised at both ends.

Clear the TX-RAI Condition

Step 1 Complete the "Clear the TX-AIS Condition" procedure on page 2-150.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.255 UNEQ-P

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: STSMON, STSTRM

An SLMF UNEQ Path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

The alarm could result from an incomplete circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.

Note If a newly created circuit has no signal, an UNEQ-P alarm is reported on the OC-3 ports and the "AIS-P" condition on page 2-21 is reported on the terminating ports. These alarms clear when the circuit carries a signal.

Clear the UNEQ-P Alarm

Step 1 In node view, click **View > Go to Network View**.

Step 2 Right-click the alarm to display the Select Affected Circuits shortcut menu.

Step 3 Click **Select Affected Circuits**.

Step 4 When the affected circuits appear, look in the Type column for VTT, which indicates a VT tunnel circuit. A VT tunnel with no VTs assigned could be the cause of an UNEQ-P alarm.

Step 5 If the Type column does not contain VTT, there are no VT tunnels connected with the alarm. Go to Step 7.

Step 6 If the Type column does contain VTT, attempt to delete these rows by completing the following steps:

Note The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

a. Click the VT tunnel circuit row to highlight it. Complete the "Delete a Circuit" procedure on page 2-164.

b. If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.

c. If any other columns contain VTT, repeat Step 6.

Step 7 If all ONS 15310-CL or ONS 15310-MA nodes in the ring appear in the CTC network view, determine whether the circuits are complete by completing the following steps:

a. Click the **Circuits** tab.

b. Verify that PARTIAL is not listed in the Status column of any circuits.

Step 8 If you find circuits listed as incomplete, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic. For specific procedures to use the test set equipment, consult the manufacturer.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 9 If the incomplete circuits are not needed or are not passing traffic, delete the incomplete circuits.

Complete the "Delete a Circuit" procedure on page 2-164.

Step 10 Recreate the circuit with the correct circuit size. Refer to the "Create Circuits" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Step 11 Log back in and verify that all circuits terminating in the reporting port are active by completing the following steps:

a. Click the **Circuits** tab.

b. Verify that the **Status** column lists all circuits as active.

Step 12 If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Step 13 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.256 UNEQ-V

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: VT-MON, VT-TERM

An SLMF UNEQ VT alarm indicates that the node is receiving SONET path overhead with Bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is not the node raising the alarm, but the node transmitting the VT signal to it. The V in UNEQ-V indicates that the failure has occurred at the VT layer.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the UNEQ-V Alarm

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-151.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15310-CL or ONS 15310-MA.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.7.257 UNQUAL-PPM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: PPM

The Unqualified PPM Inserted condition occurs when a PPM with a nonqualified product ID is plugged into the card's port; that is, the PPM passes the security code check as a Cisco PPM but is not qualified for use on the particular card.

Clear the UNQUAL-PPM Condition

Step 1 Obtain the correct Cisco PPM and replace the existing PPM with the new one.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.258 VCG-DEG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: VCG

The VCAT Group Degraded alarm is a VCAT group alarm. The condition occurs when one member circuit carried by the ML-100T-8 Ethernet card is down. This condition is accompanied by the "OOU-TPT" alarm on page 2-120. It only occurs when a Critical (CR) alarm, such as LOS, causes a signal loss.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the VCG-DEG Condition

Step 1 Look for and clear any Critical (CR) alarms that apply to the errored card or port.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.259 VCG-DOWN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: VCG

The VCAT Group Down alarm is a VCAT group alarm. The condition occurs when both member circuits carried by the ML-100T-8 Ethernet card are down. This condition occurs in conjunction with another Critical (CR) alarm.

Note For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Clear the VCG-DOWN Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-154.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.260 WKSWPR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN, STSMON, VT-MON

The Working Switched To Protection condition occurs when a line experiences the "LOS (OCN)" alarm on page 2-106.

This condition is also raised when you use the FORCE SPAN or MANUAL SPAN command at the network level. WKSWPR is visible on the network view Alarms, Conditions, and History tabs.

Clear the WKSWPR Condition

Step 1 Complete the "Clear the LOS (OCN) Alarm" procedure on page 2-106.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.7.261 WTR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN, STSMON, VT-MON

The Wait To Restore condition occurs when the "WKSWPR" condition on page 2-155 is raised and the wait-to-restore time has not expired, meaning that the active protect path cannot revert to the working path. The condition clears when the timer expires and traffic switches back to the working path.

Note WTR is an informational condition. It does not require troubleshooting.

2.8 DS-1 Line Alarms

The 15310-CL-CTX, DS1-28/DS3-EC1-3, and DS1-84/DS3-EC1-3 card DS1 ports provide three line types: ESF, D4, or Unframed. The choice of framing format determines the line alarms that the card reports. Table 2-13 lists the line alarms reported under each format. The choice of framing format does not affect the reporting of STS alarms.

Table 2-13 DS-1 Alarms by Line Type

Alarm	UNFRAMED	D4	ESF
LOS	Yes	Yes	Yes
AIS	Yes	Yes	Yes
LOF	No	Yes	Yes
IDLE	No	Yes	Yes
RAI	No	Yes	Yes
Terminal Lpbk	Yes	Yes	Yes

Table 2-13 DS-1 Alarms by Line Type (continued)

Alarm	UNFRAMED	D4	ESF
Facility Lpbk	Yes	Yes	Yes
FE Lpbk	No	No	Yes
FE Common Equipment Failure	No	No	Yes
FE Equipment Failure-SA	No	No	Yes
FE LOS	No	No	Yes
FE LOF	No	No	Yes
FE AIS	No	No	Yes
FE IDLE	No	No	Yes
FE Equipment Failure-NSA	No	No	Yes

2.9 Traffic Card LED Activity

ONS 15310-CL and ONS 15310-MA card LED behavior patterns are listed in the following sections.

2.9.1 Typical Controller Card or Ethernet Card LED Activity After Insertion

When a traffic card is inserted, the following LED activities occur:

1. The ACT LED blinks once and turns off for 5 to 10 seconds.
2. The ACT LED turns on.

2.9.2 Typical Card LED Activity During Reset

When a traffic card is inserted, the following LED activities occur:

1. The ACT LED blinks once and turns off for 5 to 10 seconds.
2. The ACT LED turns on.

2.10 Frequently Used Alarm Troubleshooting Procedures

This section provides procedures that are frequently used when troubleshooting alarms. Most of these procedures are summarized versions of more detailed procedures found in the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*. They are included in this chapter for the user's convenience. For further information, please refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Procedure Guide*.

2.10.1 Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port and span switching and switch-clearing commands, as well as lock-ons and lockouts.

Initiate a 1+1 Protection Port Force Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Force switch.

Caution The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Note A Force command switches traffic on a working path even if the path has SD or SF conditions. A Force switch does not switch traffic on a protect path. A Force switch preempts a Manual switch.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the Protect/Standby port, click this port.

Step 4 In the Switch Commands area, click **Force**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group says “Force to working” in the Selected Groups area.

Initiate a 1+1 Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.

Note A Manual command switches traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.

Step 4 In the Switch Commands area, click **Manual**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group now says “Manual to working” in the Selected Groups area.

Clear a 1+1 Force or Manual Switch Command

Note If the 1+1 protection group is configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. In revertive operation, the traffic always switches back to working. There is no revert to the protect. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Note If the Force Switch was user-initiated, the reversion occurs immediately when the clear command is issued. The five-minute WTR period is not needed in this case. If the Force was system-initiated, allow the five-minute waiting period (during WTR) before the reversion occurs.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, choose the protection group containing the port you want to clear.

Step 3 In the Selected Group area, choose the port you want to clear.

Step 4 In the Switching Commands area, click **Clear**.

Step 5 Click **Yes** in the Confirmation Dialog box.

The Force switch is cleared. Traffic immediately reverts to the working port if the group was configured for revertive switching.

Initiate a Lock-On Command

Note For ONS 15310-MA 1:1 electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group where you want to apply a lock-on.

Step 3 If you determine that the protect card is in standby mode and you want to apply the lock-on to the protect card, make the protect card active if necessary:

- **a.** In the Selected Group list, click the protect card.
- **b.** In the Switch Commands area, click **Force**.

Step 4 In the Selected Group list, click the active card where you want to lock traffic.

Step 5 In the Inhibit Switching area, click **Lock On**.

Step 6 Click **Yes** in the confirmation dialog box.

Initiate a Card or Port Lockout Command

Note For ONS 15310-MA 1:1 electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to lock out.

Step 3 In the Selected Group list, click the card where you want to lock out traffic.

Step 4 In the Inhibit Switching area, click **Lock Out**.

Step 5 Click **Yes** in the confirmation dialog box.

The lockout has been applied and traffic is switched to the opposite card.

Clear a Lock-On or Lockout Command

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to clear.

Step 3 In the Selected Group list, click the card you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock-on or lockout is cleared.

Initiate an ONS 15310-MA 1:1 Card Switch Command

Note The Switch command only works on the Active card, whether it is working or protect. It does not work on the Standby card.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group that contains the card you want to switch.

Step 3 Under Selected Group, click the active card.

Step 4 Next to Switch Commands, click **Switch**.

The working slot should change to Working/Standby and the protect slot should change to Protect/Active.

Initiate a Force Switch for All Circuits on a Path Protection Span

This procedure forces all circuits in a UPSR from the working span to the protect. It is used to remove traffic from a card that originates or terminates UPSR circuits.

Caution The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Step 1 Log into a node on the network.

Step 2 In node view, choose **Go to Network View from the View menu**.

Step 3 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the UPSR circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 4 Click the **Perform Path Protection span switching** field.

Step 5 Choose **Force Switch Away** from the drop-down list.

Step 6 Click **Apply**.

Step 7 In the Confirm UPSR Switch dialog box, click **Yes**.

Step 8 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.

Initiate a Manual Switch for All Circuits on a Path Protection Span

This procedure manually switches all circuits in a UPSR from the working span to the protect. It is used to remove traffic from a card that originates or terminates UPSR circuits.

Caution The Manual command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the UPSR circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform Path Protection span switching** field.

Step 4 Choose **Manual** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm Path Protection Switch dialog box, click **Yes**.

Step 7 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is Manual. Unprotected circuits do not switch.

Initiate a Lockout for All Circuits on a Protect Path Protection Span

This procedure prevents all circuits in a UPSR working span from switching to the protect span. It is used to keep traffic off cards that originate or terminate UPSR circuits.

Caution The Lock Out of Protect command overrides normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the UPSR circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform Path Protection span switching** field.

Step 4 Choose **Lock Out of Protect** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm Path Protection Switch dialog box, click **Yes**.

Step 7 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.

Clear an External Switching Command on a Path Protection Span

Note If the ports terminating a span are configured as revertive, clearing a Force or Manual switch to protect moves traffic back to the working port. If ports are not configured as nonrevertive, clearing a Force switch to protect does not move traffic back.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the UPSR circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Initiate a Force switch for all circuits on the span:

a. Click the **Perform Path Protection span switching** field.

b. Choose **Clear** from the drop-down list.

c. Click **Apply**.

d. In the Confirm Path Protection Switch dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is Clear. Unprotected circuits do not switch.

2.10.2 CTC Card Resetting and Switching

Caution Avoid soft resetting more than one ONS 15310-MA card at a time. Instead, issue a soft reset command for a single card, then wait until CTC shows the card is back up. You can then issue a soft reset on another card if needed. Completing soft resets in sequence helps to avoid unexpected traffic hits.

Soft- or Hard-Reset an Ethernet or Electrical Card in CTC

Note The hard-reset option is enabled on CE-100T-8 and ML-100T-8 cards only when the card is placed in the OOS-MA,MT service state.

Note Hard-resetting a traffic card causes a traffic hit in the ONS 15310-CL or ONS 15310-MA. To preserve traffic flow, perform a traffic switch in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 as appropriate.

Note Soft-resetting an ML-100T-8 Ethernet traffic card causes a traffic hit. To preserve traffic flow, perform a traffic switch in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 as appropriate. Soft-resetting a CE-100T-8 card is errorless. For more information about Ethernet cards, refer to the *Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, position the cursor over the card slot reporting the alarm.

Step 3 Right-click the card. Choose **Hard-Reset Card** or **Soft-Reset Card** from the shortcut menu.

Step 4 Click **Yes** in the Resetting Card dialog box.

Soft- or Hard-Reset a Controller Card

Caution Hard-resetting a 15310-CL-CTX or CTX2500 card can cause a traffic hit. A soft reset causes a traffic hit only if a provisioning change or firmware upgrade has occurred (or in the multiple soft-reset circumstance previously noted). To preserve traffic flow, perform a traffic switch in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 as appropriate.

Note The reset options are enabled only in the OOS-MA,MT service state.

Note Before you reset the 15310-CL-CTX or CTX2500 card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click the active 15310-CL-CTX or CTX2500 card in CTC.

Step 3 Choose **Hard-Reset Card** or **Soft-Reset Card** from the shortcut menu.

Caution Hard-resetting a 15310-CL-CTX or CTX2500 card can cause a traffic hit. A soft reset causes a traffic hit only if a provisioning change or firmware upgrade has occurred. This can be traffic-affecting. To preserve traffic flow, perform a traffic switch in the "2.10.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-156 as appropriate.

Note The hard-reset option is enabled only when the card is placed in the OOS-MA,MT service state.

Step 4 Click **Yes** in the Confirmation Dialog box.

If you performed a hard reset, the connection to the node is lost. CTC switches to network view.

Step 5 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "2.9.2 Typical Card LED Activity During Reset" section on page 2-156.

2.10.3 Physical Card Reseating and Replacement

Remove and Reinsert (Reseat) a Card

Step 1 Open the card ejectors.

Step 2 Slide the card halfway out of the slot along the guide rails.

Step 3 Slide the card all the way back into the slot along the guide rails.

Step 4 Close the ejectors.

Physically Replace a Card

Step 1 Open the card ejectors.

Step 2 Slide the card out of the slot.

Step 3 Open the ejectors on the replacement card.

Step 4 Slide the replacement card into the slot along the guide rails.

Step 5 Close the ejectors.

2.10.4 Generic Signal and Circuit Procedures

Verify the Signal BER Threshold Level

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the card reporting the alarm to display the card view.

Step 3 For the ONS 15310-CL, click the **Provisioning > Optical > Line** tabs. For the ONS 15310-MA, click the **Provisioning > DS1** or **DS3** tabs.

Step 4 Under the **SD BER** (or **SF BER**) column in the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.

Step 5 If the entry is consistent with the original provisioning, go back to your original procedure.

Step 6 If the entry is not consistent with what the system was originally provisioned for, click the cell to display the range of choices and click the original entry.

Step 7 Click **Apply**.

Delete a Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Circuits** tab.

Step 3 Click the circuit row to highlight it and click **Delete**.

Step 4 Click **Yes** in the Delete Circuits dialog box.

Verify or Create Node DCC Terminations

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Provisioning > Comm Channels > SDCC** tabs.

Step 3 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.

Step 4 If necessary, create a DCC termination by completing the following steps:

- **a.** Click **Create**.
- **b.** In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.
- **c.** In the port state area, click the **Set to IS** radio button.

d. Verify that the Disable OSPF on Link check box is unchecked.

e. Click **OK**.

Clear an OC-N Port Facility or Terminal Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the 15310-CL-CTX or CTX2500 card in CTC to display the card view.

Step 3 Click the **Maintenance > Optical > Loopback > Port** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.

Step 6 In the Admin State column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Clear an OC-N Port XC Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

Step 3 Click the **Maintenance > Optical > Loopback > SONET STS** tabs.

Step 4 Uncheck the **XC loopback** check box.

Step 5 Click **Apply**.

Clear a DS-3 or DS-1 Port Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the 15310-CL-CTX or CTX2500 card in CTC to display the card view.

Step 3 Click the **Provisioning > DS3** or the **Maintenance > DS1** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.

Step 6 In the Admin State column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Clear an EC-1 Port Loopback

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

Step 3 Click the **Maintenance > EC1 > Loopback** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.

Step 6 In the Admin State column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Clear an Ethernet Card Loopback Circuit

This procedure applies to CE-100T-8 or ML-100T-8 cards.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

Step 3 Click the **Maintenance > Loopback** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.

Step 6 In the Admin State column, determine whether any port row shows a state other than IS, for example, OOS,MT.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Note If ports managed into IS administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

CHAPTER 3

Transient Conditions

This chapter gives a description, entity, Simple Network Management Protocol (SNMP) number, and SNMP trap for each commonly encountered Cisco ONS 15310-CL and Cisco ONS 15310-MA transient condition.

3.1 Transients Indexed By Alphabetical Entry

Table 3-1 alphabetically lists all ONS 15310-CL and ONS 15310-MA transient conditions and their entity, SNMP number, and SNMP trap.

Note The Cisco Transport Controller (CTC) default alarm profile might contain conditions that are not currently implemented but are reserved for future use.

Table 3-1 ONS 15310-CL and ONS 15310-MA Transient Condition Alphabetical List

Transient Condition	Entity	SNMP Number	SNMP Trap
3.3.1 ADMIN-DISABLE, page 3-4	NE	5270	disableInactiveUser
3.3.2 ADMIN-DISABLE-CLR, page 3-4	NE	5280	disableInactiveClear
3.3.3 ADMIN-LOCKOUT, page 3-4	NE	5040	adminLockoutOfUser
3.3.4 ADMIN-LOCKOUT-CLR, page 3-4	NE	5050	adminLockoutClear
3.3.5 ADMIN-LOGOUT, page 3-5	NE	5020	adminLogoutOfUser
3.3.6 ADMIN-SUSPEND, page 3-5	NE	5340	suspendUser
3.3.7 ADMIN-SUSPEND-CLR, page 3-5	NE	5350	suspendUserClear
3.3.8 AUD-ARCHIVE-FAIL, page 3-5	EQPT	6350	archiveOfAuditLogFailed
3.3.9 DBBACKUP-FAIL, page 3-5	EQPT	3724	databaseBackupFailed
3.3.10 DBRESTORE-FAIL, page 3-5	EQPT	3726	databaseRestoreFailed
3.3.11 EFM-ERR-FRM, page 3-6	ML100T, ML1000, MLFX, ML2	6800	efmLinkMonitoringErroredFrameEvent

Table 3-1 ONS 15310-CL and ONS 15310-MA Transient Condition Alphabetical List (continued)

Transient Condition	Entity	SNMP Number	SNMP Trap
3.3.12 EFM-FRM-PER, page 3-6	ML100T, ML1000, MLFX, ML2	6810	efmLinkMonitoringErroredFramePeriodEvent
3.3.13 EFM-FRM-SEC, page 3-6	ML100T, ML1000, MLFX, ML2	6820	efmLinkMonitoringErroredFrameSecondsSummary
3.3.14 EFM-RLBK-FAIL, page 3-6	ML100T, ML1000, MLFX, ML2	6830	efmRemoteLoopbackRequestFailed
3.3.15 EFM-SYM-PER, page 3-6	ML100T, ML1000, MLFX, ML2	6790	efmLinkMonitoringErroredSymbolPeriodEvent
3.3.16 FIREWALL-DIS, page 3-6	NE	5230	firewallHasBeenDisabled
3.3.17 FRCDWKSWBK-NO-TRFSW, page 3-7	OCN	5560	forcedSwitchBackToWorkingResultedInNoTrafficSwitch
3.3.18 FRCDWKSWPR-NO-TRFSW, page 3-7	OCn	5550	forcedSwitchToProtectResultedInNoTrafficSwitch
3.3.19 INTRUSION, page 3-7	NE	5250	securityIntrusionDetUser
3.3.20 INTRUSION-PSWD, page 3-7	NE	5240	securityIntrusionDetPwd
3.3.21 LOGIN-FAIL-LOCKOUT, page 3-7	NE	5080	securityInvalidLoginLockedOutSeeAuditLog
3.3.22 LOGIN-FAIL-ONALRDY, page 3-7	NE	5090	securityInvalidLoginAlreadyLoggedOnSeeAuditLog
3.3.23 LOGIN-FAILURE-PSWD, page 3-7	NE	5070	securityInvalidLoginPasswordSeeAuditLog
3.3.24 LOGIN-FAILURE-USERID, page 3-8	NE	3722	securityInvalidLoginUsernameSeeAuditLog
3.3.25 LOGOUT-IDLE-USER, page 3-8	—	5110	automaticLogoutOfIdleUser
3.3.26 MANWKSWBK-NO-TRFSW, page 3-8	OCN	5540	manualSwitchBackToWorkingResultedInNoTrafficSwitch
3.3.27 MANWKSWPR-NO-TRFSW, page 3-8	OCN	5530	manualSwitchToProtectResultedInNoTrafficSwitch
3.3.28 PM-TCA, page 3-8	—	2120	performanceMonitorThresholdCrossingAlert
3.3.29 PS, page 3-8	EQPT	2130	protectionSwitch

Table 3-1 ONS 15310-CL and ONS 15310-MA Transient Condition Alphabetical List (continued)

Transient Condition	Entity	SNMP Number	SNMP Trap
3.3.30 RMON-ALARM, page 3-9	—	2720	rmonThresholdCrossing Alarm
3.3.31 RMON-RESET, page 3-9	—	2710	rmonHistoriesAndAlarms ResetReboot
3.3.32 SESSION-TIME-LIMIT, page 3-9	NE	6270	sessionTimeLimitExpired
3.3.33 SFTWDOWN-FAIL, page 3-9	EQPT	3480	softwareDownloadFailed
3.3.34 USER-LOCKOUT, page 3-9	NE	5030	userLockedOut
3.3.35 USER-LOGIN, page 3-9	NE	5100	loginOfUser
3.3.36 USER-LOGOUT, page 3-9	NE	5120	logoutOfUser
3.3.37 WORK-QUEUE-FULL, page 3-10	EQPT		
3.3.38 WKSWBK, page 3-10	EQPT, OCN	2640	switchedBackToWorking
3.3.39 WKSWPR, page 3-10	2R, TRUNK, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, VT-MON	2650	switchedToProtection
3.3.40 WRMRESTART, page 3-10	NE	2660	warmRestart

3.2 Trouble Notifications

The ONS 15310-CL and ONS 15310-MA systems report trouble by using standard condition characteristics that follow the rules in Telcordia GR-253 and graphical user interface (GUI) state indicators.

The ONS 15310-CL and ONS 15310-MA use standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and reports status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that you need to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

3.2.1 Condition Characteristics

Conditions include any problem detected on ONS 15310-CL and ONS 15310-MA shelves. They can include standing or transient notifications. You can retrieve a snapshot of all currently raised conditions on the network, node, or card in the CTC Conditions window or by using the RTRV-COND commands in Transaction Language One (TL1).

Note Some cleared conditions are found on the History tab.

For a comprehensive list of conditions, refer to the *Cisco ONS SONET TL1 Command Guide*.

3.2.2 Condition States

The History tab state (ST) column indicates the disposition of the condition, as follows:

- A raised (R) event is active.
- A cleared (C) event is no longer active.
- A transient (T) event is automatically raised and cleared in CTC during system changes such as user login, log out, and loss of connection to node view. Transient events do not require user action.

3.3 Transient Conditions

This section lists in alphabetical order all the transient conditions encountered in Software Release 9.0. The description, entity, SNMP number, and SNMP trap accompany each condition.

3.3.1 ADMIN-DISABLE

The Disable Inactive User (ADMIN-DISABLE) condition occurs when the administrator disables the user or the account is inactive for a specified period.

This transient condition does not result in a standing condition.

3.3.2 ADMIN-DISABLE-CLR

The Disable Inactive Clear (ADMIN-DISABLE-CLR) condition occurs when the administrator clears the disable flag on the user account.

This transient condition does not result in a standing condition.

3.3.3 ADMIN-LOCKOUT

The Admin Lockout of User (ADMIN-LOCKOUT) condition occurs when the administrator locks a user account.

This transient condition does not result in a standing condition.

3.3.4 ADMIN-LOCKOUT-CLR

The Admin Lockout Clear (ADMIN-LOCKOUT-CLR) condition occurs when the administrator unlocks a user account or the lockout time expires.

This transient condition does not result in a standing condition.

3.3.5 ADMIN-LOGOUT

The Admin Logout of User (ADMIN-LOGOUT) condition occurs when the administrator logs off a user session.

This transient condition does not result in a standing condition.

3.3.6 ADMIN-SUSPEND

The Suspend User (ADMIN-SUSPEND) condition occurs when the password for a user account expires.

This transient condition does not result in a standing condition.

3.3.7 ADMIN-SUSPEND-CLR

The Suspend User Clear (ADMIN-SUSPEND-CLR) condition occurs when the user or administrator changes the password.

This transient condition does not result in a standing condition.

3.3.8 AUD-ARCHIVE-FAIL

The Archive of AuditLog Failed (AUD-ARCHIVE-FAIL) condition occurs when the software fails to archive the audit log. The condition normally occurs when the user refers to an FTP server that does not exist or uses an invalid login while trying to archive. The user must log in again using the correct user name, password, and FTP server details.

This transient condition does not lead to a standing condition.

3.3.9 DBBACKUP-FAIL

The Database Backup Failed (DBBACKUP-FAIL) condition occurs when the system fails to back up the database when the backup command is initiated.

This condition can occur when the server is not able to handle the backup operation due to network or server issues. Repeat the same operation again and check to see if it is successful. If the backup fails, it could be due to a network issue or software program failure.

3.3.10 DBRESTORE-FAIL

The Database Restore Failed (DBRESTORE-FAIL) condition occurs when the system fails to restore the backed up database when the restore command is initiated.

This condition can be due to server issues, network issues, or human error (pointing to a file that does not exist, wrong file name, etc.). Retrying the database restore with the correct file will usually succeed. If the network issue persists, you must contact network lab support.

3.3.11 EFM-ERR-FRM

The EFM Link Monitoring - Errored Frame Event condition occurs when the number of error frames detected on the remote NE crosses the configured threshold for a configured period or time interval, and the remote NE notifies the local NE of the threshold crossing.

This transient condition does not result in a standing condition.

3.3.12 EFM-FRM-PER

The EFM Link Monitoring - Errored Frame Period Event condition occurs if the remote NE detects a specified number of errored frames which is above a configured threshold for a configured period (which is number of received frames). If so, the remote NE notifies the local NE of the exceeded threshold. This event is intended to notify user interfaces on the local NE.

3.3.13 EFM-FRM-SEC

The EFM Link Monitoring - Errored Frame Seconds Summary condition occurs when the number of errored frame seconds (a 1-second interval wherein at least one frame error was detected) on the remote NE crosses the configured threshold for a configured period or time interval. The remote NE notifies the local NE of the threshold crossing.

3.3.14 EFM-RLBK-FAIL

The EFM - Remote Loopback Request Failed condition occurs when a prior request fails. When the user triggers a remote loopback request on the local NE, the request is forwarded to the remote NE. If the remote NE does not respond to the request and the local NE times out, this condition notifies the user on the local NE about the failure.

This transient condition does not result in a standing condition.

3.3.15 EFM-SYM-PER

The EFM Link Monitoring - Errored Symbol Period Event condition occurs when the symbol errors detected at the remote NE crosses a configured threshold. This condition notifies the user on the local NE of this state.

This transient condition does not result in a standing condition.

3.3.16 FIREWALL-DIS

The Firewall Has Been Disabled (FIREWALL-DIS) condition occurs when you provision the firewall to Disabled.

This transient condition does not result in a standing condition.

3.3.17 FRCDWKSWBK-NO-TRFSW

The Forced Switch Back to Working Resulted in No Traffic Switch (FRCDWKSWBK-NO-TRFSW) condition occurs when you perform a Force Switch to the working port/card and the working port/card is already active.

This transient condition might result in a Force Switch (Ring or Span) standing condition.

3.3.18 FRCDWKSWPR-NO-TRFSW

The Forced Switch to Protection Resulted in No Traffic Switch (FRCDWKSWPR-NO-TRFSW) condition occurs when you perform a Force Switch to the protect port/card, and the protect port/card is already active.

This transient condition does not result in a standing condition.

3.3.19 INTRUSION

The Invalid Login Username (INTRUSION) condition occurs when you attempt to log in with an invalid user ID.

This transient condition does not result in a standing condition.

3.3.20 INTRUSION-PSWD

The Security Intrusion Attempt Detected (INTRUSION -PSWD) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

3.3.21 LOGIN-FAIL-LOCKOUT

The Invalid Login–Locked Out (LOGIN-FAIL-LOCKOUT) condition occurs when you attempt to log into a locked account.

This transient condition does not result in a standing condition.

3.3.22 LOGIN-FAIL-ONALRDY

The Security: Invalid Login–Already Logged On (LOGIN-FAIL-ONALRDY) condition occurs when you attempt to log into a node where you already have an existing session and a Single-User-Per-Node (SUPN) policy exists.

This transient condition does not result in a standing condition.

3.3.23 LOGIN-FAILURE-PSWD

The Invalid Login–Password (LOGIN-FAILURE-PSWD) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

3.3.24 LOGIN-FAILURE-USERID

The Invalid Login–Username (LOGIN-FAILURE-USERID) condition occurs when a user login (CTC, Cisco Transport Manager [CTM], or TL1) fails because the login username is not present on the node database. You must log in again with an existing user ID.

This transient condition is equivalent to a security warning. You must check the security log (audit log) for other security-related actions that have occurred.

3.3.25 LOGOUT-IDLE-USER

The Automatic Logout of Idle User (LOGOUT-IDLE-USER) condition occurs when a user session is idle for too long (the idle timeout expires) and the session terminates as a result. You must log in again to restart your session.

3.3.26 MANWKSWBK-NO-TRFSW

The Manual Switch Back To Working Resulted in No Traffic Switch (MANWKSWBK-NO-TRFSW) condition occurs when you perform a Manual switch to the working port/card and the working port/ card is already active.

This transient condition does not result in a standing condition.

3.3.27 MANWKSWPR-NO-TRFSW

The Manual Switch to Protect Resulted in No Traffic Switch (MANWKSWPR-NO-TRFSW) condition occurs when you perform a Manual switch to the protect port/card and the protect port/card is already active.

This transient condition does not result in a standing condition.

3.3.28 PM-TCA

The Performance Monitor Threshold Crossing Alert (PM-TCA) condition occurs when network collisions cross the rising threshold for the first time.

3.3.29 PS

The Protection Switch (PS) condition occurs when the traffic switches from a working/active card to a protect/standby card.

3.3.30 RMON-ALARM

The Remote Monitoring Threshold Crossing Alarm (RMON-ALARM) condition occurs when the remote monitoring (RMON) variable crosses the threshold.

3.3.31 RMON-RESET

The RMON Histories and Alarms Reset Reboot (RMON-RESET) condition occurs when the time-of-day settings on the 15310-CL-CTX or CTX2500 card are increased or decreased by more than five seconds. This invalidates all the history data and RMON must restart. It can also occur when you reset a card.

3.3.32 SESSION-TIME-LIMIT

The Session Time Limit Expired (SESSION-TIME-LIMIT) condition occurs when a login session exceeds the time limit and you are logged out of the session. You must log in again.

3.3.33 SFTWDOWN-FAIL

The Software Download Failed (SFTDOWN-FAIL) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support.

3.3.34 USER-LOCKOUT

The User Locked Out (USER-LOCKOUT) condition occurs when the system locks an account because of a failed login attempt. To proceed, the administrator must unlock the account or the lockout time must expire.

3.3.35 USER-LOGIN

The Login of User (USER-LOGIN) condition occurs when you begin a new session by verifying your User ID and password.

This transient condition does not result in a standing condition.

3.3.36 USER-LOGOUT

The Logout of User (USER-LOGOUT) condition occurs when you stop a login session by logging out of your account.

This transient condition does not result in a standing condition.

3.3.37 WORK-QUEUE-FULL

The Work Queue Full(WORK-QUEUE-FULL) condition occurs when the netTask Queue in VxWorks has filled up and task operations for the card are postponed.

This transient condition does not result in a standing condition.

3.3.38 WKSWBK

The Switched Back to Working (WKSWBK) condition occurs when traffic switches back to the working port/card in a nonrevertive protection group.

This transient condition does not result in a standing condition.

3.3.39 WKSWPR

The Switched to Protection (WKSWPR) condition occurs when traffic switches to the protect port/card in a nonrevertive protection group.

This transient condition does not result in a standing condition.

3.3.40 WRMRESTART

The Warm Restart (WRMRESTART) condition occurs when the node restarts while it is powered up. A restart can be caused by provisioning, such as database-restore and IP changes, or software defects. A WRMRESTART is normally accompanied by MANRESET or AUTORESET to indicate whether the reset was initiated manually (MAN) or automatically (AUTO).

This is the first condition that appears after a 15310-CL-CTX or CTX2500 card is powered up. The condition changes to COLD-START if the 15310-CL-CTX or CTX2500 card is restarted from a power loss.

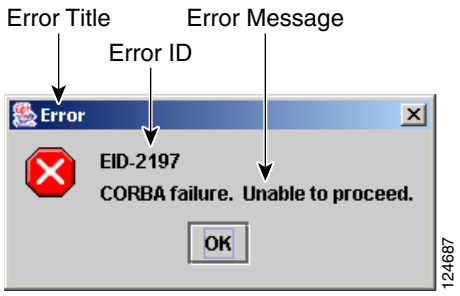
CHAPTER 4

Error Messages

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter lists the Cisco ONS 15454, 15454 SDH, 15600, 15327, 15310-CL and 15310-MA error messages. The error dialog box in Figure 4-1 consists of three parts: the error title, error ID, and error message. The table lists two types of messages: error messages (EID-*nnnn*) and warning messages (WID-*nnnn*). Error messages are alerts that an unexpected or undesirable operation has occurred which either indicates the risk of loss of traffic or an inability to properly manage devices in the network. Warnings are alerts that the requested operation could lead to an error. Warnings are sometimes used to convey important information.

Figure 4-1 Error Dialog Box



Note Some of the error messages display a **More Details** button. You can save these details to a text file using the **Save** button.

Table 4-1 gives a list of all error or warning message numbers, the messages, and a brief description of each message.

Table 4-1 Error Messages

Error/Warning ID	Error/Warning Message	Description
EID-0	Invalid error ID.	The error ID is invalid.
EID-1	A null pointer encountered in {0}.	Cisco Transport Controller (CTC) encountered a null pointer in the area described by the specified item.
EID-1000	The host name of the network element cannot be resolved to an address.	Refer to the error message text.
EID-1001	Unable to launch CTC due to applet security restrictions. Please review the installation instructions to make sure that the CTC launcher is given the permissions it needs. Note that you must exit and restart your browser in order for the new permissions to take effect.	Refer to the error message text.
EID-1002	The host name (e.g., for the network element) was successfully resolved to its address, but no route can be found through the network to reach the address.	The node is not reachable from CTC client station.
EID-1003	An error was encountered while attempting to launch CTC. {0}	Unexpected exception or error while launching CTC from the applet.
EID-1004	Problem Deleting CTC Cache: {0} {1}	Unable to delete the CTC cached JARs, because another application may have the JAR files running; for example, another instance of CTC.
EID-1005	An error occurred while writing to the {0} file.	CTC encountered an error while writing to log files, preference files, etc.
EID-1006	The URL used to download {0} is malformed.	The URL used to download the specified JAR file is incorrect.
EID-1007	An I/O error occurred while trying to download {0}.	An input or output exception was encountered when CTC tried to download the specified JAR file.
EID-1018	Password shall not contain the associated user-ID.	The password is invalid.
EID-1019	Could not create {0}. Please enter another filename.	CTC could not create the file due to an invalid filename.
EID-1020	Fatal exception occurred, exiting CTC. Unable to switch to the Network view.	CTC was unable to switch from the node or card view to the network view and is now shutting down.
EID-1021	Unable to navigate to {0}.	CTC was unable to display the requested view (node or network).
EID-1022	An IOS session cannot be opened right now with this slot. Most likely someone else (using a different CTC) already has a session opened with this slot. Please try again later.	Refer to the error message text. Ensure that the shell access in CTC (Provisioning>Security>Access) is set to non-secure mode.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-1023	This IOS session has been terminated. Terminations are caused when the session has timed out, the card resets, there is already a session with the slot, or password configuration is required.	Refer to the error message text.
EID-1025	Unable to create Help Broker.	CTC was unable to create the help broker for the online help.
EID-1026	Error found in the Help Set file.	CTC encountered an error in the online help file.
EID-1027	Unable to locate help content for Help ID: "{0}".	CTC was unable to locate the content for the help ID.
EID-1028	Error saving table. {0}	There was an error while saving the specified table.
EID-1031	CTC cannot locate the online user manual files. The files may have been moved, deleted, or not installed. To install online user manuals, run the CTC installation wizard on the software or documentation CD.	Refer to the error message text.
EID-1032	CTC cannot locate Acrobat Reader. If Acrobat Reader is not installed, you can install the Reader using the CTC installation wizard provided on the software or documentation CD.	Refer to the error message text.
EID-1035	CTC experienced an I/O error while working with the log files. Usually this means that the computer has run out of disk space. This problem may or may not cause CTC to stop responding. Ending this CTC session is recommended, but not required.	Refer to the error message text.
WID-1036	WARNING: Deleting the CTC cache may cause any CTC running on this system to behave in an unexpected manner.	Refer to the warning message text.
EID-1037	Could not open {0}. Please enter another filename.	Invalid file name. CTC is unable to open the specified file. Ensure that the file exists and the filename was typed correctly.
EID-1038	The file {0} does not exist.	The specified file does not exist.
EID-1039	The version of the browser applet does not match the version required by the network element. Please close and restart your browser in order to launch the Cisco Transport Controller.	Refer to the error message text.
WID-1041	An error occurred while closing the {0} connection.	CTC encountered an error while closing the specified connection.
WID-1042	You have selected Java version {0}. This version is outside of the recommended range and may cause an unpredictable behavior of the software. Do you wish to continue?	Refer to the warning message text.
EID-1043	Error writing to file: {0}. This might be caused by a directory permission, quota or disk volume full issue.	Check for possible causes and try again.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-1044	Warning: there is a discrepancy in the build timestamp between the NE cached jar file ({0}) and the NE ({1}). Your CTC jar cache should be emptied.	Refer to the warning message text.
EID-1046	Selected CTC version ({0}) must be greater than or equal{to the login NE version ({1}).	The CTC Software version must be greater than or equal to the Software version on the node being managed.
EID-1047	No additional Pseudo IOS windows may be opened at this time. The maximum number of Pseudo IOS windows are open.	Refer to the error message text.
EID-1048	This Pseudo IOS connection has been terminated. Terminations are caused when the session has timed out, the node resets, or when the exit command has been invoked. This may also occur when the maximum number of concurrent Pseudo IOS connections has been reached.	Refer to the error message text.
EID-1049	A Pseudo IOS connection cannot be opened right now on this node. Please try again later.	Refer to the error message text.
EID-2001	No rolls were selected. {0}	No rolls were selected for the bridge and roll.
EID-2002	The roll must be completed or canceled before it can be deleted.	You cannot delete the roll unless it has been completed or cancelled.
EID-2003	An error occurred while deleting the roll. {0}	There was an error when CTC tried to delete the roll.
EID-2004	No Cisco IOS slot was selected.	You did not select a Cisco IOS slot.
EID-2005	CTC cannot find the online help files for {0}. The files might have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs.	CTC cannot find the online help files for the specified window. The files might have been moved, deleted, or not installed. To install online help, run the setup program on the software CD.
EID-2006	An error occurred while editing the circuit(s). {0} {1}.	An error occurred when CTC tried to open the circuit for editing.
EID-2007	The preferences could not be saved.	CTC cannot save the preferences.
EID-2008	The circuit preferences could not be saved: {0}	CTC cannot find the file needed to save the circuit preferences.
EID-2009	CTC was unable to download the package: {0}	Refer to the error message text.
EID-2010	An error occurred while deleting the destination.	CTC could not delete the destination.
EID-2011	The circuit could not be destroyed.	CTC could not destroy the circuit.
EID-2012	The reverse circuit could not be destroyed.	CTC could not reverse the circuit destroy.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2013	The circuit creation failed. The circuit creation cannot proceed due to changes in the network which affected the circuit(s) being created. The dialog box will close. Please try again.	Refer to the error message text.
EID-2014	No circuit(s) were selected. {0}	You must select a circuit to complete this function.
EID-2015	The circuit {0} cannot be deleted because it has one or more rolls.	You must delete the rolls in the circuit before deleting the circuit itself.
EID-2016	The circuit deletion failed.	CTC could not delete the tunnel as there are circuits that use the tunnel.
EID-2017	An error occurred while mapping the circuit. {0}	There was an error mapping the circuit.
EID-2018	The circuit roll failed. The circuit must be in the DISCOVERED state in order to perform a roll.	There was a failure in circuit roll. Change the circuit state to DISCOVERED and proceed.
EID-2019	The circuit roll failed. Bridge and roll is not supported on DWDM circuits.	Refer to the error message text.
EID-2020	The circuit roll failed. The two circuits must have the same direction.	Refer to the error message text.
EID-2021	The circuit roll failed. The two circuits must have the same size.	Refer to the error message text.
EID-2022	The circuit roll failed. A maximum of two circuits can be selected for a bridge and roll operation.	Refer to the error message text.
EID-2023	CTC was unable to create a new user account.	Refer to the error message text.
EID-2024	An error occurred during node selection.	There was an error during node selection.
EID-2025	This feature cannot be used. Verify that each endpoint of this circuit is running software that supports this feature.	Refer to the error or warning message text. For example, this error is generated from the node view Provisioning> WDM-ANS> tabs to indicate that the selected ring type is not supported by the endpoints of the circuit. Another example is the Provisioning> VLAN tabs in card view (Ethernet card only), where it indicates that the back-end spanning tree protocol (STP) disabling is not supported.
EID-2026	The {0} request could not be applied. {1}	Error occurred while attempting to switch a path protection circuit away from a span.
EID-2027	An error occurred while deleting the circuit drop.	CTC could not delete the circuit drop.
EID-2028	An error occurred while removing the circuit node.	CTC could not remove the circuit node.
EID-2029	The requested operation is not supported.	The task you are trying to complete is not supported by CTC.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2030	An error occurred during provisioning.	There was an error during provisioning.
EID-2031	An error occurred while adding the node.	There was an error while adding a node.
EID-2032	The circuit could not be renamed. {0}	CTC could not rename the circuit.
EID-2033	An error occurred during validation. {0}	There was an internal error while validating the user changes after the Apply button was pressed. This error can occur in the Edit Circuit dialog box or in the BLSR table in the shelf view (rare condition).
EID-2034	Network circuits could not be added: {0}	Refer to the error message text.
EID-2035	The source and destination nodes are not connected.	Refer to the error message text.
EID-2036	The {0} cannot be deleted. LAN Access has been disabled on this node and this {0} is needed to access the node.	You cannot delete the DCC/GCC link as it is needed to access the node.
EID-2037	The attribute for {0} cannot be found.	CTC cannot find an attribute for the specified item.
EID-2038	The protection operation is invalid.	The protection operation you tried to execute is invalid.
EID-2040	Please select a node first.	You must select a node before performing the task.
EID-2041	No paths are available on this link. Please make another selection.	You must select a link that has paths available.
EID-2042	This span is not selectable. Only the green spans with an arrow may be selected.	Refer to the error message text.
EID-2043	This node is not selectable. Only the source node and nodes attached to included spans (blue) are selectable. Selecting a selectable node will enable its available outgoing spans.	Refer to the error message text.
EID-2044	This link may not be included in the required list. Constraints only apply to the primary path. Each node may have a maximum of one incoming signal and one outgoing link.	You must select only one link going in and out of a node. Selecting more than one link is contradictory to the path selection algorithm.
EID-2045	This link may not be included in the required list. Only one outgoing link may be included for each node.	Refer to the error message text.
EID-2047	Please enter a valid value for the slot number.	There was an error due to an invalid slot number.
EID-2048	Please enter a valid value for the port number.	There was an error due to an invalid port number.
EID-2050	The new circuit could not be destroyed.	CTC could not destroy the new circuit.
EID-2051	The circuit cannot be downgraded. {0}	The specified circuit cannot be downgraded.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2052	An error occurred during circuit processing.	There was an error during the circuit processing.
EID-2054	An error occurred while selecting an endpoint.	There was an error during the endpoint selection.
EID-2055	No endpoints are available for this selection. Please make another selection.	This error occurs in the circuit creation dialog only during a race condition that has incorrectly allowed entities without endpoints to be displayed in the combination boxes.
EID-2056	A communication error occurred: {0}	An internal error occurred in Network Alarm tab while synchronizing alarms with the nodes.
EID-2059	An error occurred while deleting the node. {0}	There was an error during the node deletion.
EID-2060	No PCA circuits were found.	CTC could not find any protection channel access (PCA) circuits for this task.
EID-2061	An error occurred while provisioning the VLAN.	There was an error defining the VLAN.
EID-2062	An error occurred while deleting VLANs. No VLAN(s) were selected. Please select a VLAN.	Refer to the error message text.
EID-2063	The default VLAN cannot be deleted.	The selected VLAN is the default VLAN and cannot be deleted.
EID-2064	An error occurred while deleting VLANs. {0}	There was an error deleting the specified VLAN.
EID-2065	The profile cannot be imported. The profile "{0}" exists in the editor and the maximum number of copies (ten) exists in the editor. The import will be aborted. The profile has already been loaded eleven times.	Cannot import the profile because the profile has reached the maximum number of copies in the editor.
EID-2066	The profile could not be stored. An error occurred while writing to {0}.	CTC encountered an error while trying to store the profile.
EID-2067	An error occurred while writing to the file. {0}	CTC encountered an error while writing the specified file.
EID-2068	The alarm profile could not be loaded from the node.	CTC encountered an error trying to load the alarm profile from the node.
EID-2069	The file could not be found or an I/O exception occurred. {0}	Either the specified file was not found, or there was an input/output exception.
EID-2070	The profile could not be deleted. {0}	There was a failure in deleting the specified profile.
EID-2071	Only one column may be highlighted.	You cannot select more than one column during clone action.
EID-2072	Only one profile may be highlighted.	You cannot select more than one profile.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2073	This column is permanent and cannot be removed.	You cannot delete a permanent column.
EID-2074	Select one or more profiles.	You have not selected any profile or column. Reset operation is done by right-clicking the selected column.
EID-2075	This column is permanent and cannot be reset.	A permanent column is non resettable.
EID-2077	This column is permanent and cannot be renamed.	You cannot rename a permanent column.
EID-2078	At least two columns must be highlighted.	You cannot compare two profiles unless you select two columns.
EID-2079	The alarm types cannot be loaded into table. There are no reachable nodes from which the list of alarm types can be loaded. Please wait until such a node is reachable and try again.	Refer to the error message text.
EID-2080	The node {0} has no profiles.	The specified node does not have any profiles.
EID-2081	An error occurred while removing profile {0} from the node {1}.	There was an error while removing the specified profile from the specified node.
EID-2082	The profile {0} does not exist on the node {1}.	CTC cannot find the specified profile from the specified node.
EID-2083	An error occurred while adding profile {0} to the node {1}.	There was an error adding the specified profile to the specified node.
EID-2085	The profile selection is invalid. No profiles were selected.	You tried to select an invalid profile. Select another profile.
EID-2086	The node selection is invalid. No nodes were selected.	You tried to select an invalid node. Select another node.
EID-2087	No profiles were selected. Please select at least one profile.	Refer to the error message text.
EID-2088	The profile name is invalid.	The profile name cannot be empty.
EID-2089	Too many copies of {0} exist. Please choose another name.	Select a unique name.
EID-2090	No nodes were selected. Please select the node(s) on which to store the profile(s).	You must select one or more nodes on which you can store the profile.
EID-2091	Unable to switch to the node {0}.	CTC is unable to switch to the specified node.
EID-2092	A general exception error occurred.	CTC encountered a general exception error while trying to complete the task.
EID-2093	The name is too short. It does not have enough characters. {0}	The name must have a minimum of six characters.
EID-2094	The password and confirmed password fields do not match.	You must make sure the two fields have the same password.
EID-2095	The password is invalid. {0}	The password you entered is not allowed.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2096	The user must have a security level.	You must have an assigned security level to perform this task.
EID-2097	No user name was specified.	You did not specify a user name.
EID-2099	An error occurred while ring switching.	There was an error during the ring switch.
EID-2100	Please select at least one profile to delete.	You have not selected the profile to delete.
EID-2101	An error occurred while protection switching.	There was an error during the protection switching.
EID-2102	The forced switch could not be removed for some circuits. You must switch these circuits manually.	The forced switch could not be removed for some circuits. You must switch these circuits manually.
EID-2103	An error occurred while upgrading the span.	There was an error during the span upgrade.
EID-2104	The circuits cannot be switched back because one or both nodes are not reachable.	This error occurs during the path protection span upgrade procedure.
EID-2106	The node name cannot be empty.	You must supply a name for the node.
EID-2107	An error occurred while adding {0}. The host is unknown.	There was an error adding the specified item.
EID-2108	{0} is already in the network.	The specified item exists in the network.
EID-2109	The node is already in the current login group.	The node you are trying to add is already present in the current login group.
EID-2110	Please enter a number between 0 and {0}.	You must enter a number in the range between 0 and the specified value.
EID-2111	This node ID is already in use. Please choose another.	Select a node ID that is not in use.
EID-2113	The extension byte for the ring cannot be set. {0}	CTC cannot set the BLSR/MS-SPRing extension byte.
EID-2114	A card communication failure occurred during the operation.	This error can occur during an attempt to apply a BLSR protection operation to a line.
EID-2115	An error occurred during the operation. {0}	There was an error in applying the specified operation.
EID-2116	The extension byte setting for the ring is invalid. {0}	The extension byte set for the specified ring is invalid.
EID-2118	The ring cannot be deleted. A protection operation is set. All protection operations must be clear for ring to be deleted.	Clear all the protection operations for the ring before deleting it.
EID-2119	{0} cannot be deleted because a protection switch is in effect. Please clear any protection operations, ensure that the reversion time is not “never” and allow any protection switches to clear before trying again.	Clear all protection operations or switches before deleting the ring.
EID-2120	The following nodes could not be unprovisioned {0} Therefore you will need to delete this {1} again later.	The specified nodes could not be unprovisioned. Try deleting this BLSR or MS-SPRing later.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2121	The ring cannot be upgraded. {0}	CTC cannot upgrade the specified ring.
EID-2122	The ring speed for is inadequate for the upgrade procedure. Only {0} (or higher) {1} can be upgraded to four-fiber.	You have selected an incorrect ring speed for upgrade. Only rings within the specified parameters can be upgraded to 4-fiber BLSR.
EID-2123	Verify that the following nodes have at least two in-service ports with the same speed as the two-fiber {0}. The ports cannot serve as timing references, and they cannot have DCC terminations or overhead circuits. {1}	Nonupgradable nodes. Verify that the specified nodes have at least two IS-NR ports with the same speed as the 2-fiber BLSR. The specified ports cannot serve as a timing reference, and they cannot have data communications channel (DCC) terminations or overhead circuits.
EID-2124	You cannot add this span because it is connected to a node that already has the east and west ports defined.	Refer to the error message text.
EID-2125	You cannot add this span as it would cause a single card to host both the east span and the west span. A card cannot protect itself.	Refer to the error message text.
EID-2126	An error occurred while provisioning the OSPF area. {0}	There is an Open Shortest Path First (OSPF) area error.
EID-2127	You cannot add this span. It would cause the following circuit(s) to occupy different {0} regions on different spans: {1} Either select a different span or delete the above circuit(s).	A circuit cannot occupy different STS regions on different spans. You may add a different span or delete the specified circuit.
EID-2128	The state is invalid.	An internal error occurred while trying to remove a span from a BLSR. This alarm occurs in the network-level BLSR creation dialog box.
EID-2129	You cannot use same slot for east and west protect ports.	Refer to the error message text.
EID-2130	The ring ID value, {0}, is not valid. Please enter a valid number between 0 and 9999.	Enter a ring ID value between 0 and 9999.
EID-2131	The reversion cannot be set to INCONSISTENT.	You must select another reversion type.
EID-2135	The overhead circuit preferences could not be stored: {0}	Input/Output error. Unable to store overhead circuit preferences.
EID-2137	An error occurred during the circuit merge. {0}	There was an error while merging the circuits.
EID-2138	Not all destinations could be deleted. Please try again.	Refer to the error message text.
EID-2139	An error occurred while updating the destinations.	There was an error in updating the circuit destinations.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2143	No online help version was selected. The online help book cannot be deleted.	Select the version of online help, and proceed.
EID-2144	An error occurred while deleting the online help book(s). {0}	You cannot delete the specified online help.
EID-2145	No nodes appear to have a Cisco IOS card.	Refer to error message.
EID-2146	This is a security violation. You may only logout of your own account.	You cannot logout of an account other than your own.
EID-2147	This is a security violation. You may only change your own account.	You cannot change an account other than your own.
EID-2148	This is a security violation. You cannot delete the account under which you are currently logged in.	You cannot delete the account you are currently logged in.
WID-2149	There is no exportable content in this view.	Refer to the error message text.
WID-2150	The node {0} is not initialized. Please wait and try again.	Wait till the specified node is initialized and try again.
WID-2152	Spanning tree protection is being disabled for this circuit.	Refer to the warning message text.
WID-2153	Adding this drop will make the circuit a PCA circuit.	Refer to the warning message text.
WID-2154	Monitor circuits cannot be created on a port grouping circuit.	Refer to the warning message text.
WID-2155	Switch counts might not be fully supported on some nodes. {0}	The specified nodes do not support switch counts completely.
WID-2156	The manual roll mode is recommended for dual rolls. For auto dual rolls, please verify that roll to facilities are in service and error-free.	Refer to the warning message text.
WID-2157	The roll(s) cannot be completed. {0}	CTC could not complete the roll because the roll is destroyed, in an incomplete state, in a TL1_roll state, is cancelled, or is not ready to complete.
EID-2158	The roll mode is invalid. {0}	There are two roll modes: auto and manual. For a one-way circuit source roll, the roll mode must be auto and for a one- way circuit destination roll, the roll mode must be manual.
EID-2159	The roll is not ready for completion. {0}	The roll is not ready for completion.
EID-2160	The roll is not connected. {0}	Refer to error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2161	The sibling roll is not complete. {0}	One of the rolls is not completed for the dual roll. If it is auto roll, it will be completed when a valid signal is detected. If it is a manual roll, you must complete the roll from CTC if Bridge and Roll is operated from CTC, or from TL1 if Bridge and Roll is operated from TL1.
EID-2162	An error occurred during roll acknowledgement. {0}	Refer to the error message text.
EID-2163	The roll cannot be canceled. {0}	CTC cannot cancel the roll.
EID-2164	An error occurred during the roll. {0}	CTC encountered a roll error.
WID-2165	The MAC address of the node {0} has been changed. All circuits originating from or dropping at this node will need to be repaired.	Repair the circuits that originate from or drop at the specified node, with the new MAC address.
WID-2166	The node cannot be inserted into the domain because it is not initialized.	Initialize the node and proceed.
WID-2167	You have insufficient security privileges to perform this action.	You do not have the privilege to perform this action.
WID-2168	The following warnings surfaced while loading {0}. {1}	CTC encountered warnings while loading the alarm profile import file.
WID-2169	One or more of the profiles selected do not exist on one or more of the nodes selected.	The profile selected does not exist on the node. Select another profile.
WID-2170	The profile list on node {0} is full. Please delete one or more profiles if you wish to add the profile. {1}	The number of profile that can exist on a node has reached the limit. To add a profile, delete any of the existing profiles.
WID-2171	You have been logged out. Click OK to exit CTC.	Refer to the warning message text.
WID-2172	The CTC CORBA (IIOP) listener port setting of {0} will be applied on the next CTC restart.	The Internet Inter-ORB Protocol (IIOP) listener port setting for the CTC Common Object Request Broker Architecture (CORBA) will be applied on the next CTC restart.
EID-2173	The port is unavailable. The desired CTC CORBA ({0}) listener port, {1}, is already in use or you do not have permission to listen on it. Please select an alternate port.	Select an alternate port, as the current port is either in use or you do not have enough permission on it.
EID-2174	An invalid number was entered. Please check it and try again.	You entered an invalid firewall port number. Try again.
WID-2175	An extension byte mismatch occurred. {0}	There is a mismatch with the extension byte.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-2176	Not all spans have the same OSPF area ID. This will cause problems with protection switching. To determine the OSPF area for a given span, click on the span and the OSPF area will be displayed in the pane to the left of the network map.	Refer to the warning message text.
WID-2178	Only one edit pane can be opened at a time. The existing pane will be displayed.	Refer to the warning message text.
WID-2179	No update is available because the circuit has been deleted.	Refer to the warning message text.
EID-2180	The CTC initialization failed during step {0}.	CTC initialization has failed in the specified step.
EID-2181	This link cannot be included because it originates from the destination.	You must not include this link as it originates from destination of a circuit. It is against the path selection algorithm.
EID-2182	The value of {0} is invalid.	The value of the specified item is invalid.
EID-2183	The circuit roll failed. Bridge and roll is not supported on VCAT circuits.	Refer to the error message text.
EID-2184	Spanning Tree Protocol cannot be enabled on some ports because the ports have been assigned an incompatible list of VLANs. You can view the VLAN/Spanning Tree table or reassign the Ethernet port VLANs.	Refer to the error message text.
EID-2185	The VLANs on some ports cannot be assigned because they are incompatible with the Spanning Tree Protocol. You can view the VLAN/Spanning Tree table or reassign the VLANs.	Refer to the error message text.
EID-2186	The software download failed on node {0}.	The software could not be downloaded onto the specified node.
EID-2187	The ring name cannot exceed {0} characters. Please try again.	You must shorten the length of the ring name.
EID-2188	The nodes in this ring do not support alphanumeric IDs. Please use a ring ID between {0} and {1}.	The ring ID should not contain alphanumeric characters, and must be in the specified range.
EID-2189	The TL1 keyword “all” cannot be used as the ring name. Please provide another name.	Refer to the error message text.
EID-2190	Adding this span will cause the ring to contain more nodes than allowed.	You have reached the maximum number of nodes allowed.
EID-2191	The ring name must not be empty.	You must supply a ring name.
EID-2192	A valid route cannot be found for the circuit creation request.	CTC could not complete the circuit creation request either because there are no physical links, or the bandwidth of the available links are already reserved.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2193	A valid route cannot be found for the circuit drop creation request.	Refer to the error message text.
EID-2194	A valid route cannot be found for the roll creation request.	Refer to the error message text.
EID-2195	The circuit VLAN list cannot be mapped to one spanning tree. You can view the VLAN/Spanning Tree table or reassign VLANs.	Refer to the error message text.
EID-2196	CTC cannot be relaunched. {0}	There is an error relaunching CTC.
EID-2197	A CORBA failure occurred. CTC cannot proceed.	There was a CORBA failure, and the task cannot proceed. Verify the Java version.
EID-2198	CTC is unable to switch to the {0} view.	CTC is unable to switch to the specified view.
EID-2199	Login failed on {0} {1}	The login failed on the specified tasks.
EID-2200	CTC has detected a jar file deletion. The jar file was used to manage one or more nodes. This CTC session will not be able to manage those nodes and they will appear gray on the network map. It is recommended that you exit this CTC session and start a new one.	Refer to the error message text.
EID-2202	An intra-node DRI circuit must have two sources.	Intranode circuit must have two sources to be a dual ring interconnect (DRI).
EID-2203	No member was selected.	You must select a member.
EID-2204	The number of circuits must be a positive integer.	The number of circuits cannot be zero or negative.
EID-2205	The circuit type must be selected.	You must select a circuit type.
EID-2206	The profile cannot be autoselected. Please select profile(s) to store and try again.	Refer to the error message text.
EID-2207	You cannot add this span. Either the ring name is too long (that is, ring name length is greater than {0}) or the endpoints do not support alphanumeric IDs.	Reduce the length of the ring name, or remove the alphanumeric characters from the end points.
EID-2208	This is an invalid or unsupported JRE.	The version of Java Runtime Environment (JRE) is either invalid or unsupported.
EID-2209	The user name must be at least {0} characters long.	The user name must be at least of the specified character length.
EID-2210	No package name was selected.	You must select a package name.
EID-2211	No node was selected for upgrade.	You must select a node for the upgrade.
EID-2212	A protected line is not provisionable.	The protected line cannot be provisioned. Choose another line.
WID-2213	The current type or state of some drops does not allow the new circuit state of {0} to be applied to them indirectly.	The circuit state, specified by {0} cannot be applied to the selected drops.
EID-2214	The node is disconnected. Please wait until the node reconnects.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2215	An error occurred while leaving the {0} page.	There was an error while leaving the specified page.
EID-2216	An error occurred while entering the {0} page.	There was an error while entering the specified page.
EID-2217	Some conditions could not be retrieved from the network view	Refer to the error message text.
EID-2218	The bandwidth must be between {0} and {1} percent.	The bandwidth must be within the specified parameters.
EID-2219	The protection operation failed. An XC loopback was applied on the cross-connection.	As the protection operation failed, a cross-connect (XC) loopback will be applied on cross-connection.
EID-2220	The tunnel status is PARTIAL. CTC is not able to change it. Please try again later.	Refer to the error message text.
EID-2221	A valid route cannot be found for the unprotected to {0} upgrade request.	Refer to the error message text.
EID-2222	One or more of the following nodes are currently part of a four-fiber {0}. Only a single four-fiber {0} is supported per node. {1}	The nodes, specified by {1}, are already part of a 4-fiber BLSR/MS-SPRing type (specified by {0}).
EID-2223	Only one circuit can be upgraded at a time.	Refer to the error message text.
EID-2224	This link may not be included because it terminates on the source.	Refer to the error message text.
EID-2225	A valid signal could not be detected while trying to complete the roll. {0}	Roll can be completed only when a valid signal is detected. If not, the roll completion may result in an error.
EID-2226	The circuit roll failed. {0}	Refer to the error message text.
EID-2320	This VCAT circuit does not support deletion of its member circuits.	You can not delete a circuit that is a member of VCAT circuit.
EID-2321	An error occurred while deleting member circuits. {0}	Refer to the error message text.
WID-2322	Not all cross-connects from selected circuits could be merged into the current circuit. They might appear as partial circuits.	Refer to the warning message text.
EID-2323	The circuit roll failed. Bridge and roll is not supported on monitor circuits.	A monitor circuit does not support Bridge and Roll.
EID-2324	An error occurred during the circuit upgrade. {0}	Refer to the error message text.
EID-2325	You have failed {0} times to unlock this session. CTC will exit after you click OK or close this dialog box.	The maximum amount of attempts to unlock this session has been reached.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-2326	Currently, CTC does not support bridge and roll on circuits that are entirely created by TL1. To continue with bridge and roll in CTC, the selected circuits must be upgraded. Is it OK to upgrade the selected circuits and continue the bridge and roll operation?	Refer to the warning message text.
WID-2327	Currently, CTC does not support bridge and roll on circuits that are partially created by TL1. To continue with bridge and roll in CTC, the selected circuits must be upgraded. Is it OK to upgrade the selected circuits and continue the bridge and roll operation?	Refer to the warning message text.
EID-2328	An error occurred during the circuit reconfiguration. {0}	The attempt to reconfigure the specified circuit has failed.
EID-2329	{0} of {1} circuits could not be successfully created.	A few circuits could not be created.
EID-2330	An error occurred during circuit verification. The selected {0} is invalid! {1}	The selected item, specified by {0}, is invalid as per the details, specified in {1}.
EID-2331	Deleting {0} might be service affecting.	Deleting the item can affect the service of CTC.
EID-2332	A validation error occurred in row {0}. {1} hold-off timer for {2} must be between {3}-10,000 ms, in steps of 100 ms.	Refer to the error message text.
EID-2333	The SSLIOP port cannot have the same port value as IIOP port. Please change it and apply again.	Refer to the error message text.
EID-3001	An Ethernet RMON threshold with the same parameters already exists. Please change one or more of the parameters and try again.	Change a few parameters in an Ethernet remote monitoring (RMON) threshold and try again.
EID-3002	An error occurred while retrieving defaults from the node: {0}	There was an error while retrieving the defaults from the specified node.
EID-3003	The file {0} cannot be loaded.	CTC cannot load the specified file.
EID-3004	Properties cannot be loaded from the node.	Refer to the error message text.
EID-3005	NE update properties cannot be saved to the file {0}.	CTC cannot save the network element (NE) update values to the specified file.
EID-3006	NE update properties cannot be loaded from the node.	Refer to the error message text.
EID-3007	An error occurred while provisioning the {0}.	There was a provisioning error for the specified item.
EID-3008	This is not a valid card.	You cannot perform DWDM automatic node setup (ANS) from the Card view. Please navigate to the Node view and try again.
EID-3009	No {0} was selected.	Select the specified item, for example, VLAN, port, slot, etc.
EID-3010	A bidirectional optical link could not be created.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3016	The subnet address is invalid.	Refer to the error message text.
EID-3017	The subnet address already exists.	Refer to the error message text.
EID-3019	The internal subnet address is incomplete.	Enter the complete internal subnet address.
EID-3020	The subnet address cannot be the same for both TSC cards. The requested action is not allowed.	A node's internal subnet must be different from one another as each TSC is on separate ethernet buses, isolated by broadcast domains.
EID-3021	An error occurred while retrieving the diagnostics: {0}	Refer to the error message text.
EID-3022	The requested action is not allowed.	The requested action is not allowed.
EID-3023	The low order cross-connect mode could not be retrieved.	Refer to the error message text.
EID-3024	The {0} cross-connect mode could not be switched. Please verify that the type and/or number of circuits provisioned does not exceed the criterion for switching modes.	CTC cannot switch the cross-connect mode for the specified item, as the type or the number of circuits does not match with the criterion for switching modes.
EID-3025	An error occurred while retrieving thresholds.	There was an error retrieving the thresholds.
EID-3026	The send DoNotUse attribute cannot be modified.	You cannot modify the Send DoNotUse field.
EID-3027	The SyncMsg attribute cannot be modified.	You cannot modify the SyncMsg field.
EID-3028	The port type cannot be changed.	You cannot change the port type.
EID-3029	Unable to switch to the byte because an overhead change is present on this byte of the port.	Refer to the error message text.
EID-3031	An error occurred while hard-resetting the card.	There was an error while resetting card hardware.
EID-3032	An error occurred while resetting the card.	There was an error while resetting the card.
EID-3033	The lamp test is not supported on this shelf.	Refer to the error message text.
EID-3035	The cross-connect diagnostics cannot be performed	Refer to the error message text.
EID-3036	The cross-connect diagnostics test is not supported on this shelf.	The cross-connect diagnostics test is not supported on this shelf.
EID-3039	An error occurred while changing the card type.	There was an error while changing the card.
EID-3040	The card type is invalid.	The selected card type is invalid.
EID-3041	An error occurred while applying changes.	CTC is unable to create a protection group. Check if the protect port supports circuits, a timing reference, SONET SDCC, orderwire, or a test access point.
EID-3042	The flow control low value must be less than the flow control high value for all ports in the card.	Refer to the error message text.
EID-3046	The flow control watermark value must be between {0} and {1}, inclusive.	The flow control watermark value must be between the two specified values.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3047	The file {0} could not be read. Please verify the name and try again.	Refer to the error message text.
EID-3048	There is no Cisco IOS startup configuration file available to download.	CTC could not find the configuration file for IOS startup.
EID-3049	The download cannot be done at this time because an update in progress.	Refer to the error message text.
EID-3050	An error occurred while trying to save the file to your local file system.	Check whether the file already exists and cannot be over written, or there is a space constraint in the file system.
EID-3051	The configuration file has a maximum size of {0} bytes.	The size of the configuration file should not exceed the specified number of bytes.
EID-3052	An error occurred while saving the configuration file to the TCC2/TCC2P.	Refer to the error message text.
EID-3053	The value of {0} must be between {1} and {2}.	The value of the item must be between the specified values.
EID-3054	The provisioned input/output ports cannot be removed or another user is updating the card. Please try to remove these ports later.	Another user may be updating the card. You can try again later.
EID-3055	The soak maintenance pane cannot be created.	Refer to the error message text.
EID-3056	Defaults cannot be saved to the file {0}.	CTC cannot save the defaults to the specified file.
EID-3057	Default properties cannot be loaded from the node.	Refer to the error message text.
EID-3058	The file {0} does not exist.	Refer to the error message text.
EID-3059	An error occurred while refreshing.	There was an error while refreshing.
EID-3060	The ALS recovery pulse interval must be between {0} seconds and {1} seconds.	The automatic laser shutdown (ALS) Recovery Interval must be between the specified range of seconds.
EID-3061	The ALS recovery pulse duration must be between {0} seconds and {1} seconds.	The automatic laser shutdown (ALS) Recovery Duration must be between the specified range of seconds.
EID-3062	An error occurred while setting values in the table.	Refer to the error message text.
EID-3064	This is not a G1000 card.	This card is not a G1000-4 card.
EID-3065	An error occurred while attempting to create this RMON threshold: {0}	You must wait some time before you try again.
EID-3066	The sample period must be between 10 and {0}.	Refer to the error message text.
EID-3067	The rising threshold must be between 1 and {0}.	This is an invalid rising threshold entry. The valid range is from 1 to the specified value.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3068	The falling threshold must be between 1 and {0}.	This is an invalid falling threshold entry. The valid range is from 1 to the specified value.
EID-3069	The rising threshold must be greater than or equal to the falling threshold.	Refer to the error message text.
EID-3070	Error in data for ports {0} Exactly one VLAN must be marked untagged for each port. These changes will not be applied.	CTC encountered data error for the specified ports. Only one VLAN should be marked untagged for each port.
EID-3071	An error occurred while retrieving the learned address list.	Unable to retrieve the learned MAC address from the NE.
EID-3072	An error occurred while clearing the learned address.	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3073	An error occurred while clearing the selected rows.	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3074	An error occurred while clearing the learned address list by {0}.	Error encountered trying to clear the learned MAC address from either a VLAN or a port.
EID-3075	At least one row in the parameter column must be selected.	Refer to the error message text.
EID-3076	CTC lost its connection with this node. The NE Setup Wizard will exit.	Refer to the error message text.
EID-3077	No optical link was selected.	Refer to the error message text.
EID-3078	An optical link could not be created.	Refer to the error message text.
EID-3079	Defaults cannot be applied to the node. {0}	CTC cannot apply the defaults to the specified node.
EID-3080	CTC cannot navigate to the target tab. {0}	CTC cannot go to the specified target tab.
EID-3081	The port type cannot be changed.	Refer to the error message text.
EID-3082	The {0} extension byte cannot be changed.	You cannot modify the specified extension byte.
EID-3084	An error occurred while retrieving laser parameters for {0}.	There is no card, or there was an internal communications error when attempting to get the laser parameters for the card.
EID-3085	No OSC Terminations were selected	Select an OSC termination and proceed.
EID-3086	One or more Osc terminations could not be created.	Refer to the error message text.
EID-3087	The OSC termination could not be edited.	Refer to the error message text.
EID-3088	No {0} card is present to switch.	No card of the specified type is available to switch.
EID-3089	The {0} state cannot be used or changed when the {1} has failed or is missing.	You cannot use or change the specified state when the card is failed or missing.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3090	The operation cannot be performed because the {0} is {1}LOCKED_ON/LOCKED_OUT.	You cannot perform operation.
EID-3091	The operation cannot be performed because the protect card is active.	Refer to the error message text.
EID-3092	The requested action cannot be applied because the service state is invalid.	Select another service state and proceed.
EID-3093	The operation cannot be performed because the duplex pair is {0}locked.	Refer to the error message text.
EID-3094	The operation cannot be performed because no cross-connect redundancy is available.	You cannot perform the requested operation on the cross connect card without having a backup cross connect card.
EID-3095	The deletion failed because the circuit is in use	Refer to the error message text.
WID-3096	An internal communication error was encountered while retrieving laser parameters. This can happen when equipment is not present or when equipment is resetting. Check the equipment state and try to refresh the values again.	Refer to the warning message text.
EID-3097	The ring termination is in use.	The ring termination you are trying to access is in use. Try after sometime.
EID-3098	No ring terminations were selected.	Select one of the ring terminations.
EID-3099	The entered key does not match the existing authentication key.	Check the authentication key and reenter.
EID-3100	An error occurred during authentication.	There was an error in authentication. Verify that the key does not exceed the character limit.
EID-3101	The DCC metric must be between 1 and 65535.	The DCC metric should be in the range of 1 to 65535.
EID-3102	The DCC metric is invalid.	There was an invalid DCC metric.
EID-3103	The IP address {0} is invalid}.	The IP address is invalid.
EID-3104	The router priority must be between 0 and 255.	The router priority should be in the range of 0 to 255.
EID-3105	The router priority is invalid.	The router priority is invalid.
EID-3106	The hello interval must be between 1 and 65535.	The hello interval should be in the range of 1 to 65535.
EID-3107	The hello interval is invalid.	The hello interval is invalid.
EID-3109	The dead interval must be between 1 and 2147483647.	The dead interval value must be between 1 and 2147483647.
EID-3110	The dead interval must be larger than the hello interval.	Refer to the error message text.
EID-3111	The LAN transmit delay must be between 1 and 3600 seconds.	The LAN transit delay should be in the range of 1 to 3600 seconds.
EID-3112	The transmit delay is invalid.	The transmit delay is invalid.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3113	The retransmit interval must be between 1 and 3600 seconds.	The retransmit interval should be in the range of 1 to 3600 seconds.
EID-3114	The retransmit interval is invalid.	The retransmit interval is invalid.
EID-3115	The LAN metric must be between 1 and 65535.	The LAN metric should be in the range of 1 to 65535.
EID-3116	The LAN metric is invalid.	The LAN metric is invalid.
EID-3117	If OSPF is active on the LAN, no DCC area IDs may be 0.0.0.0. Please change all DCC area IDs to non-0.0.0.0 values before enabling OSPF on the LAN.	Refer to the error message text.
EID-3118	If OSPF is active on the LAN, the LAN area ID cannot be the same as the DCC area ID.	LAN must be part of a different OSPF area other than the DCC network.
EID-3119	An error occurred during validation.	CTC was unable to validate the values entered by the user. This error message is common to several different provisioning tabs within CTC (examples include the SNMP provisioning tab, the General> Network provisioning tab, the Security > Configuration provisioning tab, etc.).
EID-3120	No object of type {0} was selected for deletion.	Choose an object of the specified type to delete.
EID-3121	An error occurred while deleting {0}.	There is an error deleting the item.
EID-3122	No object of type {0} was selected to edit.	Choose an object of the specified type to edit.
EID-3123	An error occurred while editing {0}.	There was an error editing the item.
EID-3124	The {0} termination is in use. Delete the associated OSPF range table entry and try again.	Refer to the error message text.
EID-3125	No {0} terminations were selected.	No specified terminations are selected.
EID-3126	The {0} termination could not be edited.	CTC could not edit the specified termination.
EID-3127	Orderwire cannot be provisioned because the E2 byte is in use by {0}.	Refer to the error message text.
EID-3128	The authentication key cannot exceed {0} characters.	The authentication key cannot exceed the specified number of characters.
EID-3129	The authentication keys do not match!	Refer to the error message text.
EID-3130	An error occurred while creating the OSPF area virtual link.	CTC encountered an error while creating the area virtual link.
EID-3131	An error occurred while creating the OSPF virtual link.	CTC encountered an error creating the virtual link.
EID-3132	An error occurred while setting the OSPF area range: {0}, {1}, false.	CTC encountered an error while setting the area range for the specified values.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3133	The maximum number of OSPF area ranges has been exceeded.	OSPF area ranges exceeded the maximum number.
EID-3134	The area ID is invalid. Use the DCC OSPF area ID, LAN port area ID, or 0.0.0.0.	Refer to the error message text.
EID-3135	The mask is invalid.	Refer to the error message text.
EID-3136	The range address is invalid.	The range address is invalid. Try again.
EID-3137	Your request has been denied because the timing source information was updated while your changes were still pending. Please retry.	Refer to the error message text.
EID-3138	The clock source for switching is invalid.	You have selected an invalid clock source. Choose another clock.
EID-3139	A switch cannot be made to a reference of inferior quality.	Refer to the error message text.
EID-3140	A higher priority switch is already active.	You cannot switch the timing source manually when a higher priority switch is already active.
EID-3141	An attempt was made to access a bad reference.	Refer to the error message text.
EID-3142	No switch is active.	None of the switches are active.
EID-3143	An error occurred while creating the static route entry.	CTC encountered an error while a creating static route entry.
EID-3144	The maximum number of static routes has been exceeded.	The number of static routes has exceeded its limit.
EID-3145	The RIP metric must be between 1 and 15.	The Routing Information Protocol (RIP) metric should be in the range of 1 to 15.
EID-3146	The RIP metric is invalid.	Refer to the error message text.
EID-3147	An error occurred while creating the summary address.	There was an error while creating the summary address.
EID-3148	No Layer 2 domain has been provisioned.	You must provision any one of the layer 2 domain.
EID-3149	The MAC addresses could not be retrieved.	Refer to the error message text.
EID-3150	The target file {0} is not a normal file.	The specified target file is not a normal file.
EID-3151	The target file {0} is not writable.	The target file is not writable. Specify another file.
EID-3152	An error occurred while creating the protection group.	CTC encountered an error creating Protection Group.
EID-3153	The card cannot be deleted because it is in use.	Refer to the error message text.
EID-3154	An error occurred while provisioning the card: CTC cannot {0} the card.	CTC cannot perform the task on the card.
EID-3155	An error occurred while building the menu.	CTC encountered an error building the menu.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3156	An error occurred while building the menu. Cards were not found for the {0} group.	CTC encountered an error while building the menu, as cards could not be found for the specified group).
EID-3157	The selected model could not be set because of an unexpected model class: {0}.	CTC encountered an unexpected model class while trying to complete the task.
EID-3158	Probable causes: - Unable to switch, because a similar or higher priority condition exists on a peer or far-end card. - A loopback is present on the working port.	Refer to the error message text.
EID-3159[1]	An error occurred while applying the operation.	CTC encountered an error while applying this operation.
EID-3160	An error occurred while provisioning the {0}.	CTC encountered the specified error.
EID-3161	An error occurred while upgrading the ring.	An error was encountered while attempting to upgrade the BLSR. Refer to the details portion of the error dialog box for more information.
EID-3162	This protection operation cannot be set because the protection operation on the other side has been changed but not yet applied.	Refer to the error message text.
EID-3163	The data in row {0} cannot be validated.	CTC cannot validate the data for the specified row.
EID-3164	The new node ID ({0}) for ring ID {1} duplicates the ID of node {2}.	The new specified node ID for the specified ring ID is the same as another node ID.
EID-3165	The ring ID provided is already in use. Ring IDs must be unique.	Refer to the error message text.
EID-3166	An error occurred while refreshing the {0} table.	CTC encountered an error while refreshing the specified table.
EID-3167	The slot is already in use.	Refer to the error message text.
EID-3168	An error occurred while provisioning.	An error was encountered while attempting the specified provisioning operation. Refer to the details portion of the error dialog box for more information.
EID-3169	An error occurred while adding the card.	CTC encountered an error while adding the card.
EID-3170	You cannot delete this card: {0}.	Refer to the error message text.
EID-3171	An error occurred while creating the trap destination.	CTC encountered an error creating the trap destination.
EID-3172	No RMON thresholds were selected.	Select an RMON threshold.
EID-3173	The contact "{0}" cannot exceed {1} characters.	The specified contact exceeds the specified character limit.
EID-3174	The description "{0}" cannot exceed {1} characters.	The specified location exceeds the specified character limit.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3175	The operator identifier "{0}" cannot exceed {1} characters.	The specified operator identifier exceeds the specified character limit.
EID-3176	The operator specific information "{0}" cannot exceed {1} characters.	The specified operator specific information exceeds the specified character limit.
EID-3177	The node name cannot be empty.	The specified name is empty.
EID-3178	The node name "{0}" cannot exceed {1} characters.	The specified name exceeds the specified character limit.
EID-3179	The protect card is in use.	Refer to the error message text.
EID-3180	The 1+1 protection group does not exist.	Create a 1+1 protection group.
EID-3181	The Y-cable protection group does not exist.	Refer to the error message text.
EID-3182	The topology element is in use and cannot be deleted as requested.	You cannot delete the topology element which is in use.
EID-3183	An error occurred while deleting the protection group.	CTC encountered an error while deleting the protection group.
EID-3184	No {0} was selected.	You must select an item before completing this task.
EID-3185	This ring has an active protection switch operation and cannot be deleted at this time.	Refer to the error message text.
EID-3186	The node is busy: {0} is {1} and cannot be deleted as requested.	The request cannot be completed.
EID-3187	An error occurred while deleting the trap destination.	CTC encountered an error deleting the trap destination.
EID-3188	An error occurred during authentication. The password entered is invalid.	The password you entered is invalid. Enter the password again.
EID-3189	The sum of the {0} must be between {1} and {2}.	Refer to the error message text.
EID-3214	The number of high order circuits for the line could not be retrieved.	The number of High Orders (STS/STM) for the line is not available.
EID-3215	An error occurred while refreshing.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3216	The proxy port is invalid.	Refer to the error message text.
EID-3217	The statistics could not be refreshed.	CTC could not refresh statistics values.
EID-3218	The automatic node setup could not be launched.	Refer to the error message text.
EID-3219	The automatic node setup information could not be refreshed.	Failure trying to retrieve automatic node setup information.
EID-3220	An error occurred while refreshing row {0}.	Error refreshing the specified row.
EID-3222	The statistics could not be cleared.	Refer to the error message text.
EID-3225	An error occurred while refreshing the pane.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3226	The {0} termination(s) could not be deleted. {1}	Refer to the error message text.
EID-3227	A baseline could not be recorded. Performance metrics will remain unchanged.	CTC failed to set the baseline values while provisioning NE. Previous values remain unchanged.
EID-3228	The {0} termination(s) could not be created. {1}	Refer to the error message text.
EID-3229	RIP is active on the LAN. Please disable RIP before enabling OSPF.	Turn off the Routing Information Protocol (RIP) on the LAN, before enabling OSPF.
EID-3230	OSPF is active on the LAN. Please disable OSPF before enabling RIP.	Turn off the OSPF on the LAN before enabling RIP.
EID-3231	An error occurred while setting the OPR.	An error was encountered while attempting to provision the optical power received (OPR).
WID-3232	The port state cannot be indirectly transitioned because the port is still providing services. If the port state should be changed, edit it directly through port provisioning.	Edit the port state while provisioning the port.
EID-3233	The current loopback provisioning does not allow this state transition.	Refer to the error message text.
EID-3234	The current synchronization provisioning does not allow this state transition.	You cannot transition the port state to the target date while in the current synchronization state.
EID-3235	The requested state transition cannot be performed on this software version.	Refer to the error message text.
EID-3236	The database restore failed. {0}	CTC failed to restore the specified database.
EID-3237	The database backup failed. {0}	CTC failed to backup the specified database.
EID-3238	The send PDIP setting on {0} is inconsistent with the setting on the control node {1}.	The send payload defect indicator path (PDI-P) setting on the specified item should be consistent with that of the specified control node.
EID-3239	The overhead termination is invalid	Refer to the error message text.
EID-3240	The maximum number of overhead terminations has been exceeded.	Overhead terminations have exceeded the limit.
EID-3241	The {0} termination port is in use.	The specified termination port is in use. Select another port.
EID-3242	An {1} exists on the selected ports. Therefore, you must create the {0}s one by one.	The specified DCC already exists on the selected port. You can create a DCC of another type.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-3243	The port you have chosen as an {0} endpoint already supports an {1}. The port cannot support both DCCs. After the {0} is created, verify that no EOC alarms are present and then delete the {1} to complete the downgrade.	The same port can not be used by multiple DCCs.
EID-3244	An {0} exists on the selected ports. Therefore, you must create the {1}s one by one.	The specified DCC already exists on the selected port. You can create a DCC of another type.
WID-3245	The port you have chosen as an {1} endpoint already supports an {0}. The port cannot support both DCCs. After the {1} is created, verify that no EOC alarms are present and then delete the {0} to complete the upgrade.	The port selected as a DCC endpoint already supports another DCC. Refer to the warning message text.
EID-3246	The wizard was not able to validate the data. {0}	CTC encountered an error.
EID-3247	An ordering error occurred. The absolute value should be {0}.	The absolute value entered was wrong.
EID-3248	The value for the parameter {0} is invalid.	CTC changed the incorrect parameter.
EID-3249	The voltage increment value is invalid.	Refer to the error message text.
EID-3250	The power monitor range is invalid.	Refer to the error message text.
EID-3251	The requested action could not be completed. {0}	CTC could not complete the specified action.
EID-3252	No download has been initiated from this CTC session.	Refer to the error message text.
EID-3253	The reboot operation failed. {0}	Refer to the error message text.
EID-3254	An error occurred during validation. {0}	The Cisco Transport Controller (CTC) was unable to validate the values entered by the user, specified by {0}. This error message is common to several different provisioning tabs within the CTC.
EID-3255	You cannot change the timing configuration because a Manual/Force operation is in effect.	Refer to the error message text.
WID-3256	The timing reference(s) could not be assigned because one or more of the timing reference(s): - is already used and/or - has been selected twice and/or - is attempting to use the same slot twice. Please verify the settings.	Refer to the warning message text.
EID-3257	Duplicate DCC numbers are not permitted. {0}.	CTC detected more than one occurrence of the a DCC number. Remove one of them.
EID-3258	A software error occurred while attempting to download the file. Please try again later.	Refer to the error message text.
EID-3259	An error occurred while creating the FC-MR threshold.	You must create a Fibre Channel Multirate (FC_MR) card threshold.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3260	An error occurred while provisioning the internal subnet: {0}	The specified internal subnet could not be provisioned.
EID-3261	The port rate provisioning cannot be changed while circuits exist on this port.	Refer to the error message text.
EID-3262	The port provisioning cannot be changed when the port status is {0}.	You must provision the ports only when the port is Out of Service.
WID-3263	You are using Java version {0}. CTC should run with Java version {1}. It can be obtained from the installation CD or http://java.sun.com/j2se/	CTC is being launched with the wrong version of the JRE {0}. This version of CTC requires a particular version of the JRE {1}. The CTC and browser must be closed and restarted to allow the correct Java version to be loaded.
EID-3265	An error occurred while modifying the protection group.	Protection Group could not be modified.
EID-3266	Conditions could not be retrieved from the shelf or card view.	Refer to the error message text.
WID-3267	The XTC protection group cannot be modified.	Refer to the warning message text.
WID-3268	The filter entry is invalid. {0}	The specified entry is invalid.
WID-3269	The {0} operation was successfully initiated for {1} but its completion status could not be obtained from the node. When the node is accessible, check its software version to verify if the {0} succeeded.	Refer to the error message text.
WID-3270	The file {0} does not exist.	The specified file does not exist.
WID-3271	The value entered must be greater than {0}.	The value entered must be greater than the specified value.
WID-3272	An entry is required.	An entry is required to complete this task.
WID-3273	{0} already exists in the list.	The specified item already exists in the list.
WID-3274	A software upgrade is in progress. Network configuration changes that result in a node reboot cannot take place during a software upgrade. Please try again after the software upgrade is done.	Refer to the warning message text.
WID-3275	Ensure that the remote interface ID and the local interface ID on the two sides match. (The local interface ID on this node should equal the remote interface ID on the neighbor node and vice-versa).	Refer to the warning message text.
WID-3276	Both {0} and {1} exist on the same selected port. {2}	The specified port has both SDCC and LDCC.
WID-3277	The description cannot exceed {0} characters. Your input will be truncated.	The input exceeds the character limit. The value will be truncated to the maximum character limit.
WID-3279	This card has been deleted. CTC will return to the shelf view.	CTC returns to node view.
WID-3280	ALS will not engage until both the protected trunk ports detect LOS.	Refer to the warning message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-3282	Performing a software upgrade while TSC 5 is active could result in a service disruption. It is recommended that you make TSC 10 the active TSC by performing a soft reset of TSC 5. The following ONS 15600s are currently unsafe to upgrade...	Refer to the warning message text.
WID-3283	Before activating a new version, ensure that you have a database backup from the current version.	Refer to the warning message text.
WID-3284	Reverting to an older version.	CTC is being reverted to an older version of application.
WID-3285	Applying FORCE or LOCKOUT operations might result in traffic loss.	Refer to the warning message text.
WID-3286	The ring status is INCOMPLETE. CTC cannot determine if there are existing protection operations or switches in other parts of the ring. Applying a protection operation at this time could cause a traffic outage. Please confirm that no other protection operations or switches exist before continuing.	Refer to the warning message text.
WID-3287	There is a protection operation or protection switch present on the ring. Applying this protection operation now will probably cause a traffic outage.	Refer to the warning message text.
WID-3288	The status of this ring is INCOMPLETE. CTC will not be able to apply this change to all of the nodes in the {0}.	Change the ring status to apply the change to all nodes in the ring type.
EID-3290	The specified provisionable patchcord(s) could not be deleted.	Refer to the error message text.
EID-3291	The revertive behavior cannot be changed because a protection switch is active.	Protection switch should not be active to change the revertive behaviour.
EID-3292	An error occurred while resetting the shelf.	CTC encountered an error while resetting the node.
EID-3293	No such provisionable patchcords exists.	You are attempting to delete a provisionable patchcord that does not exist. This happens when multiple instances of CTC are running and attempting to delete the same provisionable patchcord concurrently.
EID-3294	No RMON thresholds are available for the selected port.	Refer to the error message text.
EID-3295	This card does not support RMON thresholds.	Refer to the error message text.
EID-3296	Buffer-to-buffer credit is only supported for Fibre Channel (FC) and FICON.	Refer to the error message text.
EID-3298	This interfaces does not support ALS auto restart.	Refer to the error message text.
EID-3300	Duplicate OSPF area IDs are not permitted.	OSPF area IDs should be unique.
EID-3301	The LAN metric cannot be zero.	Refer to the error message text.
EID-3302	The standby {0} is not ready.	Standby controller card is not ready.
EID-3303	The DCC area ID and {0} conflict. {1}	DCC Area ID and ring type, specified by {0}, conflict each other due to the details specified by {1}.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3304	The DCC number is out of range.	Enter a DCC number that is within the range
EID-3305	OSPF cannot be active on the LAN interface when the backbone area is set on a DCC interface.	You cannot have the default OSPF area on a DCC while OSPF is enabled on the LAN.
EID-3306	Ethernet circuits must be bidirectional.	Refer to the error message text.
EID-3307	An error occurred while creating a connection object at {0}.	CTC encountered an error at the specified connection while creating the connection.
EID-3308	DWDM links can be used only for optical channel circuits.	Refer to the error message text.
EID-3309	The link was excluded because it was in the wrong direction.	The optical channel (circuit) does not allow the specified link to be included because it is in the wrong optical direction.
EID-3310	The DWDM link does not have wavelengths available.	Refer to the error message text.
EID-3311	The laser is already on.	Refer to the error message text.
EID-3312	The power setpoint cannot be changed. {0} {1}	CTC cannot change the power setpoint. The new setpoint would either make the thresholds inconsistent or set the fail threshold outside the range.
EID-3313	The offset cannot be modified because the service state of the port is IS.	Refer to the error message text.
EID-3314	The requested action is not allowed. The state value is invalid.	Refer to the error message text.
EID-3315	This operation cannot be performed.	CTC is unable to perform operation.
EID-3316	The node side is invalid.	This task was applied to the wrong node side.
EID-3317	The ring name is too long.	Reduce the number of characters in the name.
EID-3318	The ring name is invalid.	The name you entered is illegal.
EID-3319	The wrong line was selected.	Select another line
EID-3320	The optical link could not be deleted.	CTC cannot delete the optical link.
EID-3321	This feature is unsupported by this version of software.	Refer to the error message text.
EID-3322	The equipment is not plugged in.	Plug-in the equipment and proceed.
EID-3323	The APC system is busy.	Automatic Power Control (APC) system is busy.
EID-3324	There is no path to regulate.	There is no circuit path to regulate.
EID-3325	The requested action is not allowed.	Generic DWDM provisioning failure message.
EID-3326	The input was invalid.	The input value is incorrect.
EID-3327	An error occurred while retrieving thresholds.	There was an error retrieving the thresholds. This message is displayed only for the OSCM/OSC-CSM line thresholds.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3328	An error occurred while applying changes to row {0}. The value is out of range.	There was an error applying the changes to the specified row. The value is out of range.
EID-3330	Unable to switch to the byte because an overhead channel is present on this byte of the port.	Refer to the error message text.
EID-3331	An error occurred while applying changes to the row.	Refer to the error message text.
EID-3334	Timing parameters on the protect port cannot be changed.	You cannot change timing parameters on protect port.
EID-3335	The port type cannot be changed because the SDH validation check failed. Check if this port is part of a circuit, protection group, SONET DCC, orderwire, or UNI-C interface.	Refer to the error message text.
EID-3336	An error occurred while reading a control mode value.	The Control Mode must be retrieved.
EID-3337	An error occurred while setting a set point gain value.	The Gain Set Point must be set.
EID-3338	An error occurred while reading a set-point gain value.	The Gain Set Point must be retrieved.
EID-3339	An error occurred while setting a tilt calibration value.	The tilt calibration must be set.
EID-3340	An error occurred while setting expected wavelength.	The expected wavelength must be set.
EID-3341	An error occurred while reading expected wavelength.	The expected wavelength must be retrieved.
EID-3342	An error occurred while reading actual wavelength.	The actual wavelength must be retrieved.
EID-3343	An error occurred while reading actual band.	The actual band must be retrieved.
EID-3344	An error occurred while reading expected band.	The expected band must be retrieved.
EID-3345	An error occurred while setting expected band.	The expected band must be set.
EID-3346	An error occurred while retrieving defaults from the node: {0}.	There was an error retrieving defaults from the specified node.
EID-3347	The file {0} cannot be loaded.	CTC cannot load the specified file.
EID-3348	Properties cannot be loaded from the node.	Refer to the error message text.
EID-3349	NE update properties cannot be saved to a file.	Check your file system for space constraint or any other problem.
EID-3350	NE update properties cannot be loaded from the node.	Refer to the error message text.
EID-3351	The file {0} does not exist.	The specified file does not exist.
EID-3352	An error occurred while setting a value at {0}.	There was an error while setting the value at the specified location.
EID-3353	No such interface is available.	The interface specified is not present in CTC.
EID-3354	The specified endpoint is in use.	Select another endpoint that is not in use.
EID-3355	The specified endpoint is incompatible.	Refer to the error message text.
EID-3357	The connections could not be calculated.	Refer to the error message text.
EID-3358	An optical link model does not exist for the specified interface.	Create an optical link model for the interface, and proceed.
EID-3359	Optical parameters could not be set for the node.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3360	ANS cannot be performed. Please check {0} parameter value.	Refer to the error message text.
EID-3361	The ring termination is in use. An error occurred while deleting the ring termination.	You cannot delete a ring in use.
EID-3362	An error occurred while deleting the ring termination.	There was an error while deleting ring termination.
EID-3363	No ring terminations were selected.	You must select a ring termination.
EID-3364	An error occurred while creating the ring ID.	There was an error while creating the ring ID.
EID-3365	The OSC termination is in use.	Select another optical service channel (OSC) which is not in use.
EID-3366	The OSC termination could not be deleted.	There was an error deleting the OSC termination.
EID-3370	No optical link was selected.	You must select an optical link.
EID-3371	An error occurred while calculating the automatic optical link list.	Refer to the error message text.
EID-3372	CTC attempted to access an OCHNC connection that has been destroyed.	CTC destroyed an external attempt to access an optical channel network connection.
EID-3375	The expected span loss must be set.	Refer to the error message text.
EID-3376	The measured span loss could not be retrieved.	Refer to the error message text.
EID-3377	The wrong interface was used.	The interface used for the card is wrong.
EID-3378	This is a duplicate origination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the origination node.
EID-3379	This is a duplicate termination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the remote node.
EID-3380	The host cannot be found.	Refer to the error message text.
EID-3381	The maximum frame size must be between {0} and {1} and may be increased in increments of {2}.	The frame size must be in the specified range. This can incremented by the specified value.
EID-3382	The number of credits must be between {0} and {1}.	The number of credits must be between the specified values.
EID-3383	The GFP buffers available must be between {0} and {1} and may be increased in increments of {2}.	The GFP buffers must be in the specified range. This can incremented by the specified value.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-3384	You are about to force the use of Secure Mode for this chassis. You will not be able to undo this operation. Is it OK to continue?	Refer to the warning message text.
EID-3385	{0}. Delete the circuits and try again.	Refer to the error message text.
EID-3386	The transponder mode could not be provisioned: {0}	The specified transponder mode cannot be provisioned.
EID-3387	You must change port(s) {0} to an out-of-service state before changing card parameters. Click "Reset" to revert the changes.	All the card ports should be changed to out-of-service before changing the parameters.
EID-3388	The card mode cannot be changed because the card has circuits.	Refer to the error message text.
EID-3389	An error occurred while changing the card mode.	Refer to the error message text.
EID-3390	The port is in use.	Refer to the error message text.
EID-3391	The port rate cannot be changed because the port has been deleted.	You cannot change the port rate of a card that has been deleted.
WID-3392	The timing reference(s) could not be assigned because with external timing, only a single protected, or two unprotected timing references per BITS Out can be selected. Please use the "Reset" button and verify the settings.	Refer to the warning message text.
WID-3393	The timing reference(s) could not be assigned because with line or mixed timing, only a single unprotected timing reference per BITS Out can be selected. Please use the "Reset" button and verify the settings.	Refer to the warning message text.
EID-3394	An error occurred while refreshing the power monitoring values.	Refer to the error message text.
EID-3395	The configuration is invalid. {0}	CTC encountered an error in IP address, net mask length, or default router, or a restricted IIOP port was selected.
EID-3396	The configuration is invalid. The standby controller card is not a TCC2P card.	The standby controller card should be a TCC2P card.
EID-3397	The file {0} is the wrong version.	The specified file is of wrong version.
EID-3398	The PPM cannot be deleted.	Refer to the error message text.
EID-3399	The PPM cannot be deleted because it has port(s) in use.	Remove the ports connected to the Pluggable Port Module before it can be deleted.
EID-3400	Unable to switch. A force to the primary facility is not allowed.	Refer to the error message text.
EID-3401	{0} cannot be provisioned for the port while {1} is enabled.	The relationship between parameters {0} and {1} are such that enabling either one, prevents the provisioning of the other.
EID-3402	The switch request could not be completed. The {0} card is not present or is not responding. Try again after ensuring that the {0} card is present and is not resetting.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3403	The administrative state transition has not been attempted on the monitored port.	Refer to the error message text.
EID-3404	The far end IP address could not be set on the {0} termination. The IP address cannot be: loopback (127.0.0.0/8) class D (224.0.0.0/4) class E (240.0.0.0/4) broadcast (255.255.255.255/32) internal {1}	Refer to the error message text.
EID-3405	You cannot change card parameters with port {0} in {1} state. Click “Reset” to revert the changes.	Refer to the error message text.
EID-4000	The {0} ring name cannot be changed now because a {0} switch is active.	You cannot change the ring name because a switch of the same ring type is active.
EID-4001	The {0} node ID cannot be changed now because a {0} switch is active.	You cannot change the ring ID because a switch of the same ring type is active.
WID-4002	CAUTION: Reverting to an earlier software release may result in TRAFFIC LOSS and loss of connectivity to the node. It may require onsite provisioning to recover. If the node was running {0} before, reverting will restore the {0} provisioning, losing any later provisioning. If the node was running some other version, reverting will LOSE ALL PROVISIONING. {1} {2}	Refer to the warning message text.
EID-4003	The Cisco IOS console is disabled for the card in Slot {0}.	The card may not be an IOS-based card or it may be rebooting.
EID-4004	An error occurred while canceling the software upgrade.	CTC encountered an error while cancelling the software upgrade.
EID-4005	{0} encountered while performing a database backup.	CTC encountered the specified error during database backup.
EID-4006	The file {0} does not exist or cannot be read.	Refer to error message.
EID-4007	The size of the file {0} is zero.	The size of the file that is being backed up or restored is zero.
WID-4008	A software upgrade is in progress. {0} cannot proceed during a software upgrade. Please try again after the software upgrade has completed.	The specified action cannot be performed during a software upgrade. You must try after the upgrade process is completed.
EID-4009	{0} encountered while restoring the database.	CTC encountered the specified error while restoring the database.
EID-4010	The operation was terminated because: {0}	Refer to the error message text.
EID-4011	An error occurred during provisioning: {0}	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-4012	Node management for {0} is not provided.	Refer to the warning message text.
EID-4013	CAUTION: Reverting to an earlier software release may result in TRAFFIC LOSS and loss of connectivity to the node. It may requireonsite provisioning to recover. If the node was running {0} before, reverting will restore the {0} provisioning, losing any later provisioning. If the node was running some other version, reverting will LOSE ALL PROVISIONING. {1} {2} {3}	Refer to the error message text.
EID-4014	The manual path trace mode for this equipment does not support an expected string consisting of all null characters. Please change the expected string or the path trace mode.	The path trace mode does not support strings that consist of null characters. You must either change the expected string or the path trace mode.
EID-4015	Software activation is in progress. Provisioning is not allowed.	Refer to the error message text.
EID-4016	Software activation is in progress. {0} is not allowed.	Refer to the error message text.
EID-4017	Path Trace mode cannot be set at this endpoint. The circuit is one-way.	Refer to the error message text.
WID-4018	{0} already exists. Do you want to replace it?	Refer to the warning message text.
EID-4019	Profile cannot be mapped because the UNI Port is not in transparent mode.	Refer to the error message text.
EID-4020	Profile cannot be mapped because the transparent mode UNI Port tagged VLAN is not {0}.	Refer to the error message text.
EID-4021	Profile cannot be mapped because SVLAN {0} is not enabled for the NNI Port.	Refer to the error message text.
EID-4022	The user already exists.	Refer to the error message text.
EID-4023	Access control already exists for the group selected.	Refer to the error message text.
EID-4024	The View already exists.	Refer to the error message text.
EID-4025	Invalid Mask entry, cant be more then {0} the length of OID.	Refer to the error message text.
EID-4026	CTC was unable to create a new view.	Refer to the error message text.
EID-4027	Name and Subtree OID cant be empty.	Refer to the error message text.
EID-4028	Password will be sent as plain text.	Refer to the error message text.
EID-4029	The passowrds must be at least {0} characters long.	Refer to the error message text.
EID-4030	The admitted SVLAN values must be in the range [1-4093].	Refer to the error message text.
EID-4031	On {0} interface the Recover from Fiber Cut Fails.	Refer to the error message text.
EID-5000	A valid route cannot be found for the tunnel change request.	Refer to the error message text.
EID-5001	The tunnel could not be changed.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5002	The tunnel could not be restored and must be recreated manually.	Refer to the error message text.
EID-5003	The circuit roll failed. {0}	Refer to the error message text.
EID-5004	There is already one four-fiber {0} provisioned on the set of nodes involved in {1}. The maximum number of four-fiber {0} rings has been reached for that node.	There is already one 4F BLSR provisioned on the set of nodes involved in the ring. The maximum number of 4F BLSR rings has been reached for that node.
WID-5005	A non-zero hold-off time can violate switching time standards, and should only be used for a circuit with multiple path selectors.	Refer to the warning message text.
WID-5006	Warning: A different secondary {0} node should only be used for DRI or open-ended path protected circuits.	You should use different secondary end point only for DRI or open-ended path protected circuits.
WID-5007	If you change the scope of this view, the contents of this profile editor will be lost.	Refer to the warning message text.
WID-5008	Please ensure that all the protection groups are in proper states after the cancellation.	Refer to the warning message text.
WID-5009	The circuit {0} is not upgradable. No {1} capable {2}s are available at the node {3}.	No VT capable STSs are available at the node.
EID-5010	The domain name already exists.	Refer to the error message text.
EID-5011	The domain name cannot exceed {0} characters.	You may have reached the maximum number of characters.
WID-5012	The software load on {0} does not support the addition of a node to a 1+1 protection group.	Refer to the warning message text.
EID-5013	{0} does not support the bridge and roll feature. Please select a different port.	The specified port does not support Bridge and Roll.
EID-5014	An automatic network layout is already in progress. Please wait for it to complete before running it again.	You must for the automatic network layout to complete before running it again.
WID-5015	{0} cannot be applied to {1}.	You cannot apply the admin state operation, specified by {0}, to port count, specified by {1}.
EID-5016	An error occurred while attempting to provision the {0}. {1}	CTC encountered an error while provisioning the card.
EID-5017	Provisioning could not be rolled back. The {0} might be left in an INCOMPLETE state and should be manually removed.	You may have to remove the BLSR manually as it was left incomplete.
EID-5018	{0} is a(n) {1} node and cannot be added to a(n) {2} network.	You cannot add the node {0} of type {1} to the host node of type {2}. This prevents you from hosting both SONET and SDH nodes in the same session.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5019	The manual path trace mode for this equipment does not support an expected string consisting of all null characters. Please change the expected string or the path trace mode.	The path trace mode does not support strings that consist of null characters. You must either change the expected string or the path trace mode.
EID-5020	Software activation is in progress. Provisioning is not allowed.	Refer to the warning message text.
EID-5021	Software activation is in progress. {0} is not allowed.	Refer to the error message text.
WID-5022	Warning: Ethergroup circuits are stateless (that is, always in service). The current state selection of {0} will be ignored.	Refer to the warning message text.
EID-5023	CTC cannot communicate with the node. The operation failed.	CTC encountered a network communication error. Connectivity between CTC and the NE was disrupted, either transiently or permanently.
EID-5024	The overhead circuit will not be upgraded.	Refer to the error message text.
WID-5025	The path targeted for this switch request is already active. The switch request can be applied, but traffic will not switch at this time.	Refer to the warning message text.
EID-5026	An ONS 15600 cannot serve as the primary or secondary node in a four-fiber {0} circuit. Please change your ring and/or node selections so that an ONS 15600 is not chosen as the primary or secondary node in this four-fiber {1} circuit.	Refer to the error message text.
WID-5027	The {0} Edit dialog box for the ring {1} has been closed due to significant provisioning changes. These changes might only be transitory, so you can reopen the {0} Edit dialog box to view the updated state.	Re-open the BLSR/MS-SPRing edit window to view the updated state of the ring.
WID-5028	Warning: This operation should only be used to clean up rolls that are stuck. It might also affect completeness of the circuit. Is it OK to continue with the deletion?	Refer to the warning message text.
EID-5029	A software downgrade cannot be performed to the selected version while an SSXC card is inserted in this shelf. Please follow the steps to replace the SSXC with a CXC card before continuing the software downgrade.	Refer to the error message text.
EID-5030	A software downgrade cannot be performed at the present time.	Try the software downgrade later.
WID-5031	Canceling a software upgrade during a standby TSC clock acquisition might result in a traffic outage.	Refer to the warning message text.
EID-5032	An error occurred while accepting the load.	Refer to the error message text.
EID-5033	The profile could not be loaded. An error occurred while decoding the characters.	CTC detected an error while decoding characters and could not load the profile.
EID-5034	The profile could not be loaded. An error occurred while trying to recognize the file format.	CTC detected an error and could not load the profile.
EID-5035	The profile could not be loaded. An error occurred while reading the file.	CTC could not read the file and is therefore unable to load the profile.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5036	The GNE hostname {0} is invalid.	The specified host name is invalid. CTC could not resolve the host name to any valid IP address
EID-5037	Provisionable patchcords cannot be created between transponder trunk ports and multiplexer/demultiplexer ports on the same node.	You must create provisionable patchcords between transponder trunk ports and mux/demux ports that are on different nodes.
EID-5038	Provisionable patchcords created between transponder trunk ports and multiplexer/demultiplexer ports must use the same wavelength: {0} is not equal to {1}.	Wavelengths used by provisionable patchcords for transponder trunk ports and mux/demux ports must be the same.
EID-5039	Provisionable patchcords created between transponder trunk ports and multiplexer/demultiplexer ports must use the same wavelength: {0} is not equal to {1}. Please provision the {2} wavelength on {3}.	Transmitter and receiver port wavelengths are not equal. Provision the receiver and transmitter wavelengths on transmitter and receiver ports respectively.
EID-5040	Provisionable patchcords created between OC3/OC12 ports and multiplexer/demultiplexer ports are not supported.	Refer to the error message text.
EID-5041	Provisionable patchcords created between gray OC-N trunk ports and multiplexer/demultiplexer ports are not supported.	Refer to the error message text.
EID-5042	Provisionable patchcords created between OC-N trunk ports and multiplexer/demultiplexer ports must use the same wavelength: {0} is not equal to {1}.	Wavelengths used by provisionable patchcords for OC-N trunk ports and mux/demux ports must be the same.
WID-5043	Warning: Only the line card was provisioned. The wavelength compatibility check was skipped.	Refer to the warning message text.
EID-5044	Virtual links can be used only for OCH-Trail circuits.	Refer to the error message text.
EID-5045	The virtual link does not have wavelengths available.	Set wavelengths for the virtual link and proceed.
WID-5046	Warning: if you select “Use OCHNC Direction,” your circuit will be limited to nodes prior to release 07.00.	Refer to the warning message text.
EID-5047	Provisionable patchcords created between OC3/OC12 ports are not supported.	Refer to the error message text.
EID-5048	Provisionable patchcords created between gray OC-N trunk ports are not supported.	Refer to the error message text.
EID-5049	Provisionable patchcords created between gray OC-N trunk ports and multiplexer/demultiplexer ports are not supported.	Refer to the error message text.
EID-5050	The element model could not be found. {0}	The specified Element Model cannot be located.
WID-5051	The port state cannot be indirectly transitioned because the port aggregates OCHCC circuits: if the port state needs to be changed, edit it directly through port provisioning.	Refer to the warning message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5052	The operation is not valid for the connection type.	You may have selected the incorrect switch.
EID-5053	The operation cannot be performed because the connection is under test access.	Refer to the error message text.
EID-5054	The TL1 tunnel could not be opened. {0}	Refer to the error message text.
EID-5055	Some patchcords were not deleted. Patchcords cannot be deleted if they are incomplete or support any circuits, or if the nodes supporting them are not connected.	Refer to the error message text.
EID-5056	This PPC cannot be deleted because one or more circuits are provisioned over it.	Remove the circuits provisioned over the provisionable patchcord before trying to delete it.
EID-5057	The addition of the last node has not yet finished. Please wait before trying to add a new node.	Refer to the error message text.
EID-5058	An OCHNC upgrade is applicable only to bidirectional circuits.	Refer to the error message text.
EID-5059	The OCHNC upgrade failed. One or more communication failures occurred during the operation.	CTC encountered a complete failure while upgrading optical channel network connection.
EID-5060	The OCHNC upgrade partially failed. One or more communication failures occurred during the operation. Create the OCHCC manually.	CTC encountered a partial failure while upgrading an optical channel network connection.
EID-5061	The overhead circuit source and destination must reside on the same shelf.	Refer to the error message text.
EID-5062	A four-fiber {0} cannot be created using three cards.	A four-fiber BLSR needs four cards.
WID-5063	The profile "{0}" includes a change to the OPEN-SLOT alarm severity. This change is disallowed for the ONS 15600. "{1}" will continue to use the OPEN-SLOT severity of MN that is included in the default configuration. Other changes from the "{2}" profile were successfully applied to {3}".	Refer to the warning message text.
EID-5064	{0} {1}	This indicates the status of path protection switching.
WID-5065	If you apply routing constraints to more than {0} nodes, performance might be affected and the operation might require more time than expected. Select Yes if you intend to proceed in spite of this risk, or No if you prefer to review your selection.	Refer to the warning message text.
WID-5066	The routing constraints will be lost. Are you sure you want to reset your changes?	Refer to the warning message text.
WID-5067	The routing constraints will be lost. Are you sure you want to leave this panel?	Refer to the warning message text.
EID-5068	The routing constraints could not be applied.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5069	A source node cannot be added to either of these lists.	Select a node other than the source node to add to the route.
EID-5070	A destination node cannot be added to either of these lists.	Select a node other than the destination node to add to the route.
EID-5071	This node already belongs to one of these lists.	The node is already selected either in include or exclude list in the OCH circuit.
EID-5072	An OCH-Trail tunnel link was found but without any associated circuit.	Create an OCH-Trail circuit associated with the link.
EID-5073	You are creating an unprotected link from a protected port. Do you want to continue?	Refer to the error message.
EID-5074	Deleting OCH DCN circuits will cause a loss of connectivity to nodes in the circuit path that do not have other DCN connections. Do you want to continue?	Refer to the error message.
EID-5075	The VLAN ID must be a number between 1 and 4093.	Enter a number between 1 and 4093.
EID-5076	An error occurred while provisioning the VLAN ID. The VLAN ID is already present in the current profile	Select a VLAN ID that is not present in the current profile.
EID-5077	An error occurred while provisioning the VLAN database profile. {0}	CTC could not save the VLAN profile to the file name mentioned.
EID-5078	The VLAN merge is not complete. You forgot to fill {0} record(s).	Fill in the number of records specified and then proceed.
EID-5079	An error occurred while validating the provisionable patchcord.	Refer to the error message text.
EID-5080	No rolls are available.	You cannot delete a roll without selecting a roll.
EID-5081	An error occurred while tracing the RPR ring: {0}	The circuit reference is invalid.
EID-5082	{0} does not support: - Low-order circuits that have both {1}-protected and {2}-protected spans and that cross a node that does not have low-order cross-connect capability. - High-order circuits that carry low-order circuits with the parameters described above.	Refer to the error message text.
EID-5083	This circuit is not the same size as the existing circuit {0}. This circuit has size {1} and the existing circuit has size {2}.	During an RPR circuit creation ML card, the new circuit size and the existing circuit size must be the same.
EID-5084	The Trunk model could not be found. {0}	The trunk specified is not found.
EID-5085	The maximum number of VLAN DB profiles is {0}.	Refer to the error message.
EID-5086	The circuit roll failed. You cannot bridge and roll the selected circuit because it has a monitor circuit.	Refer to the error message.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5087	You cannot use same slot for east working and west protect ports.	Refer to the error message text.
EID-5088	You cannot use same slot for east working and west protect ports.	Refer to the error message text.
WID-5089	The maximum number of circuits that can be deleted at a time is 200. Do you want to delete the first 200 circuits selected?	Refer to the error message text
EID-5090	This operation cannot be completed. The selected circuits have different state models; please select circuits of the same type.	Refer to the error message text
EID-5091	Some PPC terminations were not repaired.	Refer to the error message text
WID-5092	The TL1 encoding mode for the tunnel is being changed. Do you want to modify the encoding?	Confirm if you really want to modify TL1 tunnel encoding.
EID-6000	This platform does not support power monitoring thresholds.	Refer to the error message text.
EID-5094	Currently, CTC does not support bridge and roll on circuits having multiple cross-connects on a single node.	Refer to the error message text.
EID-5095	No path were selected. Please select at least one path starting from the {0} NE.	Refer to the error message text.
EID-5096	The first path must starts from the {0} NE.	Refer to the error message text.
EID-5097	The selected path should be linked with the last selected and keep the same direction.	Refer to the error message text.
EID-5098	The node is not selectable. Only the Span between the nodes are selectable.	Refer to the error message text.
EID-5099	Raman Command Error on {0}. {1}.	Refer to the error message text.
EID-5100	Raman Command in TimeOut. {0}.	Refer to the error message text.
EID-5101	Failed to get trunk ports for client. {0}.	Refer to the error message text.
EID-5102	Protected cards must have 2 trunk ports. (found {0}).	Refer to the error message text.
EID-5103	Failed to get colocated OCH ports for trunk: {0}.	Refer to the error message text.
EID-5104	Both OCHCC and OCHNC Protected are not allowed.	Refer to the error message text.
EID-5105	Cannot find entity model for endpoint: {0}.	Refer to the error message text.
EID-5106	Cannot find Out OTS line for selected endpoint: {0}.	Refer to the error message text.
EID-5107	Cannot find Protected Out OTS line for selected endpoint: {0}.	Refer to the error message text.
EID-5108	The demultiplexer associated with the selected endpoint :{0} is missing or not connected.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5109	The demultiplexer associated with the protect path for the selected endpoint: {0} is missing or not connected.	Refer to the error message text.
EID-5110	The card selection is invalid. No cards were selected.	Refer to the error message text.
EID-5111	An error was occurred while configuring SNMPv3 proxy server.	Refer to the error message text.
EID-5112	No source of trap was selected.	Refer to the error message text.
EID-5113	Specify a valid value for target tag.	Refer to the error message text.
EID-5114	Specify a valid value for context engine ID.	Refer to the error message text.
EID-5115	No value was selected for proxy type.	Refer to the error message text.
EID-5116	No value was selected for local user.	Refer to the error message text.
EID-5117	No value was selected for proxy destination.	Refer to the error message text.
EID-5118	Specify a valid value for target IP.	Refer to the error message text.
EID-5119	The password for authentication should be at least 8 characters long.	Refer to the error message text.
EID-5120	The user name should be atleast 6 characters long.	Refer to the error message text.
EID-5122	The node ({0}) does not support ML-MR POS port protection.	Refer to the error message text.
EID-5123	Primary ({0}) and secondary ({1}) nodes have to be the same for ML-MR POS port protection.	Refer to the error message text.
EID-5124	No nodes appear to support a Pseudo IOS connection.	Refer to the error message text.
EID-5125	No node was selected.	Refer to the error message text.
EID-5126	The Pseudo IOS console is disabled for the selected node.	Refer to the error message text.
EID-5127	The password for encryption should be at least 8 characters long.	Refer to the error message text.
EID-5128	{0} configuration already exists for the {1} {2} with the specified parameters.	Refer to the error message text.
WID-5129	Failed to retrieve the complete OSPF database as it is very large. Please contact Cisco Technical Support (http://www.cisco.com/techsupport) if you want to retrieve the complete OSPF database.	Refer to the warning message text.
EID-5130	Connection failed on node {0}	Refer to the error message text.
EID-5131	An error occurred while deleting the circuit end point.	Refer to the error message text.
WID-5132	Failed to retrieve the status of Proxy server on the node. Please contact Cisco Technical Support (http://www.cisco.com/techsupport) if you want to retrieve the Proxy status.	Refer to the warning message text.
EID-5133	SNMPv3 Proxy configuration already exists for the specified parameters.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5134	On node {0} the calculated gain is much greater than expected. The wizard cannot operate under this condition. Please call TAC for support.	Refer to the error message text.
EID-6001	One of the XC cards has failures or is missing.	Check whether all the cross-connect cards are installed and working.
EID-6002	One of the XC cards is locked.	Unlock the cross-connect card.
EID-6003	The OSC termination could not be created. This ring ID is already assigned.	Enter a new ID for the ring.
EID-6004	A system reset cannot be performed while a BLSR ring is provisioned on the node.	Remove the BLSR from the node and continue with the reset procedure.
EID-6005	The timing references could not be assigned. - Only two DS1 or BITS interfaces can be specified. - DS1 interfaces cannot be retimed and used as a reference. - BITS-2 is not supported on this platform.	Refer to the error message text.
EID-6006	The timing references could not be assigned. - An NE reference can only be used if the timing mode is LINE. - A BITS reference can only be used if the timing mode is not LINE. - A Line reference can only be used if the timing mode is not EXTERNAL.	Refer to the error message text.
EID-6008	SF BER and SD BER are not provisionable on the protect line of a protection group.	Refer to the error message text.
WID-6009	If autoadjust GFP buffers is disabled, GFP buffers available must be set to an appropriate value based on the distance between the circuit endpoints.	Refer to the warning message text.
WID-6010	If auto detection of credits is disabled, credits available must be set to a value less than or equal to the number of receive credits on the connected FC endpoint.	Refer to the warning message text.
WID-6011	Ingress idle filtering should be turned off only when required to operate with non-Cisco Fibre Channel/FICON-over-SONET equipment.	Refer to the warning message text.
EID-6012	The retiming configuration could not be changed because there are circuits on this port.	You cannot change the timing configuration on this port unless the circuits on this port are deleted.
EID-6013	The NTP/SNTP server could not be changed. {1}	Refer to the error message text.
EID-6014	The operation failed because the reference state is OOS.	Change the Out-of-service state to Active.
EID-6015	The distance extension cannot be disabled if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to the error message text.
EID-6016	The card mode cannot be changed to Fibre Channel Line Rate if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6017	The destination of a {0} route cannot be a node IP address.	A node IP address cannot be the destination for a static route.
EID-6018	The destination of a {0} route cannot be the same as the subnet used by the node.	Refer to the error message text.
EID-6019	The destination of a static route cannot be 255.255.255.255	The network address such as 255.255.255.255 is not valid. Enter a valid address.
EID-6020	The destination of a static route cannot be the loopback network (127.0.0.0/8).	Refer to the error message text.
EID-6021	The subnet mask length for a non default route must be between 8 and 32.	Length of subnet mask must be within the specified range.
EID-6022	The subnet mask length for a default route must be 0.	Refer to the error message text.
EID-6023	The destination of a {0} route cannot be an internal network{1}.	The destination of a static route must not be an internal network.
EID-6024	The destination of a {0} route cannot be a class D (224.0.0.0/4) or class E (240.0.0.0/4) address.	The destination of a static route must not be a class D or class E address.
EID-6025	The destination of a {0} route cannot be a class A broadcast address (x.255.255.255/8).	The destination of a static route must not be a class A broadcast address. It should be (xxx.0.0.0).
EID-6026	The destination of a {0} route cannot be a class B broadcast address (x.x.255.255/16).	The destination of a static route must not be a class B broadcast address.
EID-6027	The destination of a {0} route cannot be a class C broadcast address (x.x.x.255/24).	The destination of a static route must not be a class C broadcast address.
EID-6028	The destination of a {0} route cannot be the subnet broadcast address associated with a node IP address.	The destination of a static route must not be a subnet broadcast address of a node IP.
EID-6029	The next hop of a static route cannot be the same as the destination of the route or an internal network{0}.	Static route must have the default route as the next hop, and not destination of the route or internal network.
EID-6030	The next hop of a static default route must be the provisioned default router.	The default route is selected for networks that do not have a specific route.
EID-6031	No more static routes can be created.	You have reached the maximum number of static routes.
EID-6032	This static route already exists.	Refer to the error message text.
EID-6033	A previous operation is still in progress.	Another operation is in progress. You must try after sometime.
EID-6035	The parent entity does not exist.	Refer to the error message text.
EID-6036	The parent PPM entity does not exist.	Create a parent entity for the PPM.
EID-6037	This equipment type is not supported.	CTC does not support this equipment.
EID-6038	The PPM port is invalid.	Refer to the error message text.
EID-6039	The card is part of a regeneration group.	Select another card.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6040	Out of memory.	Refer to the error message text.
EID-6041	The port is already present.	Refer to the error message text.
EID-6042	The port is used as timing source.	Choose another port because the selected port is being used as a timing source.
EID-6043	A DCC or GCC is present.	Refer to the error message text.
EID-6044	The card or port is part of protection group.	Refer to the error message text.
EID-6045	The port has overhead circuit(s).	Refer to the error message text.
EID-6046	The ITU-T G.709 configuration is not compatible with the data rate.	Refer to the error message text.
EID-6047	The port cannot be deleted because its service state is OOS-MA,LPBK&MT.	To delete the port, you must change the port state to OOS-DSBLD.
EID-6048	{0} is {1}.	The trunk port is in the wrong state to carry out the action.
EID-6049	The card operating mode of {0} is not supported.	CTC does not support the mode of operation requested on the card.
EID-6050	Some {0} terminations were not {1}d. {2}	Refer to the error message text.
WID-6051	All {0} terminations were {1}d successfully. {2}	Refer to the warning message text.
EID-6052	The authentication key can not be blank.	Enter an authentication key.
EID-6053	No more SNMP trap destinations can be created.	You have reached the maximum number of SNMP trap destinations.
EID-6054	{0} is not a valid IP address for an SNMP trap destination.	The IP address specified is not a valid receiver of SNMP traps.
EID-6055	The IP address is already in use.	Refer to the error message text.
EID-6056	The SNMP trap destination is invalid. {0}	The specified SNMP trap destination is invalid. Choose another destination.
WID-6057	Changing the card mode will result in an automatic reset.	Refer to the warning message text.
EID-6058	The maximum number of IP-over-CLNS tunnels has been exceeded.	Refer to the error message text.
EID-6059	The specified IP-over-CLNS tunnel already exists!	Specify another IP Over CLNS tunnel.
EID-6060	An error occurred while trying to {0} an IP-over-CLNS tunnel entry: {1}.	Refer to the error message text.
EID-6061	An error occurred while deleting the IP-over-CLNS tunnel entry.	CTC encountered an error while deleting the IP Over CLNS tunnel entry.
EID-6062	The selected IP-over-CLNS tunnel does not exist.	Create a IP Over CLNS tunnel.
EID-6063	The selected router does not exist.	Create a router.
EID-6064	The MAA address list is full.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6065	The selected area address is duplicated.	Enter another area address.
EID-6066	The primary area address cannot be removed.	Refer to the error message text.
EID-6067	The selected area address does not exist.	Choose another area address.
EID-6068	The IP-over-CLNS NSEL cannot be modified while there are IP-over-CLNS tunnel routes provisioned.	You cannot change the NSEL address if tunnels are provisioned.
EID-6069	The node is currently in ES mode. Only Router 1 can be provisioned.	An End System needs only one provisioned router.
EID-6070	No router was selected.	Select a router.
EID-6071	The TARP data cache cannot be flushed.	You cannot flush the cache in the Tunnel identifier Address Resolution Protocol (TARP) state.
EID-6072	The TARP data cache entry cannot be added: {0}	You cannot add the specified cache entry.
WID-6073	A TARP request has been initiated. Try refreshing the TARP data cache later.	Refer to the warning message text.
EID-6074	End system mode only supports one subnet.	Refer to the error message text.
EID-6075	An error occurred while trying to remove a MAT entry. The entry does not exist.	CTC is removing the MAT entry.
EID-6076	An error occurred while trying to {0} a TARP manual adjacency entry: {1}	CTC cannot add the specified adjacency entry for reasons unknown.
EID-6077	The area address must be between 1 and 13 bytes long, inclusive.	The area address should not be more than 13 characters.
EID-6078	A TDC entry with this TID {0} does not exist in the table.	The specified Tunnel Identifier does not exist.
EID-6079	A TDC entry with this TID {0} could not be removed. Please verify that TARP is enabled.	You must enable TARP in order to remove the TDC entry.
WID-6080	Router {0} does not have an area address in common with Router 1. Switching from IS L1/L2 to IS L1 in this case will partition your network.	Refer to the warning message text.
EID-6081	The limit of 10 RADIUS server entries has been reached.	CTC does not allow more than 10 RADIUS servers.
EID-6082	{0} cannot be empty.	The Shared Secrets field should not be empty.
EID-6083	The entry you selected for editing has been altered by another user. The changes cannot be committed.	Refer to the error message text.
EID-6084	The RADIUS server entry already exists.	Specify another RADIUS server entry.
WID-6085	Disabling shell access will prevent Cisco TAC from connecting to the vxWorks shell to assist users.	Refer to the warning message text.
EID-6086	The card cannot be changed because card resources are in use.	The card you are trying to remove is being used. Cannot change the card.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6087	The card cannot be changed because the card type is invalid or incompatible.	Refer to the error message text.
EID-6088	This line cannot be put into loopback while it is in use as a timing source.	Refer to the error message text.
EID-6089	The interface was not found. {0}	CTC cannot find the specified interface.
EID-6090	The interface type is not valid for this operation. {0}	Choose another interface.
EID-6091	The current state of the interface prohibits this operation. {0}	The port is in an invalid state to set a loopback.
EID-6092	This operation is prohibited for this interface. {0}	CTC does not allow this operation for the specified interface.
EID-6093	The maximum number of TARP data cache entries has been exceeded.	You have exceeded the number of characters permitted.
EID-6094	The maximum number of manual adjacency table entries has been exceeded.	Refer to the error message text.
EID-6095	The AIS/Squelch mode is invalid.	Refer to the error message text.
EID-6096	A default IP-over-CLNS tunnel route is only allowed on a node without a default static route and a default router of 0.0.0.0.	Refer to the error message text.
EID-6097	The authorization key does not comply with Cisco IOS password restrictions. {0}	Specify another authorization key.
EID-6098	A default static route is not allowed when a default IP-over-CLNS tunnel exists.	Refer to the error message text.
EID-6099	You cannot create a subnet on a disabled router.	Create the subnet on an active router.
WID-6100	Disabling a router that has a provisioned subnet is not recommended.	Refer to the warning message text.
EID-6101	The MAT entry already exists.	Refer to the error message text.
WID-6102	The new card has less bandwidth than the current card. Circuits of size VT15 and larger will be deleted.	Refer to the warning message text.
EID-6103	The TDC entry already exists.	Specify another entry for TARP Data Cache.
EID-6104	APC ABORTED.	Automatic Power Control is aborted.
EID-6105	The 'Change Card' command is valid for MRC cards only when Port 1 is the sole provisioned port.	Refer to the error message text.
EID-6106	To delete all RADIUS server entries, RADIUS authentication must be disabled.	Disable Radius authentication and proceed.
EID-6107	The node failed to restart the TELNET service on the selected port. Try using another unreserved port that is not being used within the following ranges: 23, 1001-9999 (with the exception of 1080, 2001-2017, 2361, 3081-3083, 4001-4017, 4022, 4081, 4083, 5000, 5001, 7200, 9100, 9300, 9401).	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6108	That port is already in use.	Restart a TELNET session.
EID-6109	A section trace is active on the trunk port. The action cannot be completed.	Actions such as putting the port in an incomplete state are not permitted while a section trace is active.
EID-6110	The maximum number of TARP requests has been reached.	You have exceeded the maximum number of TARP requests.
EID-6111	The card in Slot {0} cannot be removed from the protection group while its traffic is switched.	Refer to the error message text.
EID-6112	An error occurred while adding a shelf: {0}	The shelf ID specified is invalid or already exists, the equipment does not support multishelf, the specified shelf position is out of range, or the specified shelf position is already in use.
EID-6113	An error occurred while deleting a shelf: {0}	One or more of the equipment modules (provisioned virtual links, provisioned server trails, provisioned protection groups, or provisioned DCCs) in the shelf is currently in use. Delete cards from all the slots and try again.
EID-6114	The maximum number of supported shelves has already been provisioned.	Refer to the error message text.
EID-6115	There are bad or duplicate shelf positions. Valid rack numbers are {0} to {1}. Valid rack positions are {2} to {3}.	Refer to the error message text.
EID-6116	CTC attempted to access an OCH-Trail connection that has been destroyed.	Software has prevented an attempt to access an OCH trail.
EID-6117	CTC attempted to access an OCH-Trail edit that has been destroyed.	The resource cannot be accessed because it is released or fully utilized.
WID-6118	The following slots are provisioned but do not have cards installed: {0} CTC will assume they are ITU-T interfaces.	Refer to the warning message text.
EID-6119	The shelves could not be rearranged. {0}	One of the following conditions is present: duplicate shelf positions, invalid shelf positions, or concurrent movement (two CTC sessions are attempting to rearrange the shelves at the same time.)
EID-6120	This equipment does not support multishelf.	Refer to the error message text.
WID-6121	This internal patchcord cannot be provisioned because the endpoints have no compatible wavelengths.	The end points of an internal patchcord should have compatible wavelengths.
EID-6122	The wizard could not be started. {0}	CTC was unable to initiate the wizard due to the specified reason.
EID-6123	The OSI request can not be completed successfully.	A communication failure occurred.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6124	The ALS recovery pulse interval is invalid.	Refer to the error message text.
EID-6125	The ALS recovery pulse duration is invalid.	Refer to the error message text.
EID-6126	The current setting does not support the specified ALS mode.	Refer to the error message text.
EID-6127	All enabled routers are required to have the same area.	Refer to the error message text.
EID-6128	A software download is in progress. Configuration changes that result in a card reboot cannot take place during a software download. Please try again after the software download is done.	Refer to the error message text.
EID-6129	The payload configuration and card mode are incompatible.	Refer to the error message text.
EID-6135	A DCC is present.	A data communication channel (DCC) already exists.
EID-6136	An error occurred during provisioning: {0}	CTC was not able to provision the specified port or card.
EID-6137	Multishelf cannot be disabled. {0}	Multishelf is not supported on equipment, is already disabled, or modules on the shelf are currently in use.
EID-6138	The LAN configuration is invalid.	Verify the LAN configuration.
EID-6139	Invalid card(s) are present. Please remove all non-MSTP cards and try again.	Non-DWDM cards cannot be added to an a DWDM node. Remove the cards.
EID-6140	The shelf identifier for a subtended shelf cannot be provisioned through CTC. It must be changed using the LCD.	Refer to the error message text.
EID-6143	The DHCP server could not be changed.	Refer to the error message text.
EID-6144	The port provisioning cannot be changed when the port media is Undefined.	If the port is not pre-provisioned with the type of media that is going to be inserted, you cannot access any of the existing values for the port.
WID-6145	OSPF on LAN should only be enabled when the LAN routers run OSPF. Otherwise, the node will not be reachable from outside its subnet. RIP implementation only advertise routes in one direction to connected routers. It does not learn or distribute routes advertised by other routers. Also note that enabling OSPF on the LAN will temporarily cause the current list of static routes to stop being advertised to remote nodes and only be used locally.	Refer to the warning message text.
WID-6146	Deleting the protection group while in a switched state might cause a loss of traffic. It is recommended that you verify switch states before proceeding.	Refer to the warning message text.
EID-6149	The LAPD MTU size must be greater than or equal to the {0} LSP buffer size {1}. Alternatively, you can decrease the {0} LSP buffer size to {2}.	Refer to the error message text.
EID-6150	The value is out of range.	Enter a value that is within the range.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6151	The minimum span loss must be less than the maximum span loss.	Refer to the error message text.
EID-6152	The "Use NTP/SNTP Server" field is checked. Enter the NTP/SNTP server IP address or server name.	Enter the NTP/SNTP server name. To leave this field empty, uncheck the "Use NTP/SNTP Server" and proceed.
EID-6153	The maximum frame size is invalid.	Refer to the error message text.
EID-6154	To combine unidirectional two-port provisioning and autonegotiation on the same port, autonegotiation must be set first.	Refer to the error message text.
EID-6155	Transponder mode cannot be provisioned with circuits on the card.	Refer to the error message text.
EID-6156	The transponder configuration is invalid.	The transponder is not configured properly.
EID-6157	The watermark values are either out of range or inconsistent.	Enter valid watermark values.
EID-6179	The 1+1 protection group is not optimized.	Refer to the error message text.
EID-6196	The equipment has failed or is missing.	Operation is requested on a failed or missing equipment.
EID-6197	Attributes cannot be changed when the port administrative state is {0}.	You cannot change the attributes when the port is in the specified administrative state.
WID-6204	This action will cause the node to reboot. When provisioning in single-shelf mode, Shelf {0} of the node that you connect to must be properly preprovisioned or you will lose traffic. Use the LCD to return to single-shelf mode. CTC cannot be used for this. Changing from subtended shelf mode to single-shelf mode could be traffic-affecting.	Refer to the warning message text.
EID-6205	The interlink port is not provisioned.	The user creates an ADM peer group without interlink ports.
EID-6206	The ADM peer group has already been created on the peer card.	The user creates an ADM peer group involving an ADM card inserted in a peer group.
EID-6207	This card is not in the ADM peer group.	The selected ADM card is not involved in an ADM peer group.
EID-6208	The payload is not OTU2.	Refer to the error message text.
EID-6209	The side is already defined by the node.	During the creation of a side on node, a side is already defined.
EID-6210	No side was selected.	The user requests an operation on a side, but no side is selected.
EID-6211	The side was not deleted.	CTC could not delete the selected side successfully.
EID-6212	One of the ports is connected to a patchcord or virtual link.	An operation on a port was not performed because the port is connected to a patchcord or a virtual link.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6213	It is not possible to associate the side to the two ports.	During the creation of a side it is not possible to associate the selected ports to the new side.
EID-6214	The port is already assigned to a side.	The selected port is already assigned to a side.
EID-6215	Error provisioning the CVLAN ID. Enter a valid number or range between 0 and 4094.	The entered CVLAN ID was out of the admitted range.
EID-6216	Changing card will reset the optical thresholds to the default setting and may affect the optical connection. The optical connection will work only if the optical performance is compatible with {0} card. Please check the network design.	Refer to the error message text.
EID-6217	You cannot delete the {0} {1}.	You cannot delete {0} {1} because it is part of an ADM peer group or one or more circuits are provisioned on it.
EID-6218	Invalid ethernet duplex value	the Ethernet duplex value is invalid. Enter again.
EID-6219	Invalid committed info rate	The committed info rate value is invalid. Enter again.
EID-6220	Invalid mode value	The mode value is invalid. Enter again.
EID-6221	Invalid mtu value	The MTU value is invalid. Enter again.
EID-6222	Invalid flow control value	The flow control value is invalid. Enter again.
EID-6223	Invalid Network Interface Mode	The network interface mode value is invalid. Enter again.
EID-6224	Invalid ingress COS value	The ingress COS value is invalid. Enter again.
EID-6225	Invalid ethertype value	The Ethertype value is invalid. Enter again.
EID-6226	Invalid buffer size value	The Buffer size value is invalid. Enter again.
EID-6227	Invalid egress QOS value	The egress QOS value is invalid. Enter again.
EID-6228	Invalid QinQ working Mode	The QinQ working mode is invalid. Enter again.
EID-6229	Configured protection status Not Supported	The protection status is not supported
EID-6230	The number of provisioned entries exceeds the limit	Refer to the error message text.
EID-6231	This is not a valid VLAN ID.	Entered VLAN ID is not present in the database file.
EID-6232	The VLAN remapping ID is not allowed.	Refer to the error message text.
EID-6233	The CVLAN is duplicated.	You cannot have identical CVLAN IDs.
EID-6234	The VLAN ID is out of range.	The VLAN ID entered is out of range.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6235	This is not a valid VLAN name.	The entered VLAN name exceeds the number of characters (32) allowed.
EID-6236	The protected VLAN number exceeds the maximum allowed.	The user enters more than 256 protected VLAN in the VLAN database.
EID-6237	The port is not in OOS disabled admin state	Refer to the error message text.
EID-6238	The VLAN ID is in use.	The entered VLAN ID is in use by a node.
EID-6239	APC wrong node side.	Refer to the error message text.
EID-6240	You cannot change the Admin State for an interlink port when it is part of an ADM peer group. This operation is not supported.	Refer to the error message text.
EID-6242	The protection slot is invalid.	You must select a valid protection slot.
EID-6243	The {0} address of {1} is invalid.	Refer to the error message text.
EID-6244	The mask of {0} is invalid.	The mask of the specified value is not valid.
EID-6245	The cost must be between 1 and 32767.	Refer to the error message text.
EID-6246	The {0} address cannot be {1}.	Refer to the error message text.
EID-6247	The authentication type is invalid.	Enter a valid authentication type.
EID-6248	The cost must between 1 and 15.	Refer to the error message text.
EID-6249	The port has a cross-connect.	Refer to the error message text.
EID-6250	The reversion time is invalid.	The reversion time is invalid. Enter again.
EID-6251	Invalid Margin For Span Aging. Value is not in the range 0 - 10.	Enter a value between 0 and 10.
EID-6252	The data cannot be retrieved because ANS parameters cannot be calculated on the node in its current configuration.	Refer to the error message text.
EID-6253	Invalid Margin For Span Aging.	Refer to the error message text.
EID-6254	SDH mode does not support timing references.	Timing reference is not supported by SDH mode.
EID-6255	Only DS1 interfaces with ESF line types support timing references.	Refer to the error message text.
EID-6256	sendDoNotUse and sendDoNotUseFF are mutually exclusive.	Refer to the error message text.
EID-6257	The termination is already in use.	Refer to the error message text.
EID-6258	The side is carrying services or traffic.	Refer to the error message text.
EID-6259	A pluggable module on Port 22 remains unmanaged.	Refer to the error message text.
EID-6260	You cannot delete this port. There was a severe architectural error related to the index of the pluggable trunk port object. Please contact technical support for assistance.	Refer to the error message text.
EID-6261	This is not a valid VLAN ID. The VLAN database is empty.	The user adds a row without a valid VLAN database loaded.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6263	The equipment requires two slots.	The user provisions a double footprint card in a single slot.
EID-6264	The patchcord is duplicated.	Refer to the error message text.
EID-6265	The wavelength is in use by an OCH trail, a virtual link, or an internal patchcord.	Refer to the error message text.
EID-6266	The card cannot be changed because the port has not been provisioned.	Refer to the error message text.
EID-6267	Each port can have a maximum of 8 MAC addresses.	Refer to the error message text.
EID-6268	This server trail does not have a valid start or end.	Refer to the error message text.
EID-6269	The maximum number of server trails is 3743.	Refer to the error message text.
EID-6270	A unique server trail ID could not be allocated.	Refer to the error message text.
EID-6271	The server trail already exists.	Refer to the error message text.
EID-6272	The server trail size must not exceed the port bandwidth.	Refer to the error message text.
EID-6273	An OCH Trail circuit is active on the trunk port. To modify the ITU-T G.709 parameter, the circuit must be out of service.	Refer to the error message text.
EID-6274	Unable to restore this database: The software version cannot be obtained from the node. Please try again.	The user tries to restore a database on a node, but its not possible to get the software version from it.
EID-6275	You cannot change this parameter. The port is part of an active circuit.	Certain parameters like Port Rate and Admin State cannot be changed when the port is part is part of an active circuit. Delete all the circuits on the port before changing admin state of the port.
EID-6276	APC is disabled. APC Correction Skipped. Override cannot be performed.	Refer to the error message text.
EID-6277	There are no alarm conditions available to run APC Correction Skipped Override.	Refer to the error message text.
EID-6278	APC Correction Skipped Override is not supported for this card.	Refer to the error message text.
EID-6279	Protection cannot be disabled when the FPAS alarm is active.	Refer to the error message text.
WID-6280	Any configuration change will be lost and the operation is traffic affecting.	Refer to the error message text.
EID-6281	The port is involved in a protection group. The protected port is not in the {0} administrative state	Change the port state to administrative.
WID-6282	Forcing FPGA update will be traffic-affecting.	Refer to the error message text.
WID-6283	Enabling ALS on a DWDM trunk port that is connected to a channel filter will result in a conflict with the ALS on the amplifier card or with the VOA startup process. Is it OK to continue?	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-6284	Changing the timing standard will re-initialize the shelf timing and might affect traffic. OK to continue?	Refer to the error message text.
WID-6285	Since you are changing the IP address of one node containing some PPC terminations, you are also requested to run the PPC Repair tool in order to fix the IP addresses stored in the nodes connected by these PPCs	Refer to the error message text.
EID-6286	The port type cannot be changed because the port has been deleted.	Refer to the error message text.
EID-6287	You cannot edit the {0} {1}.	Port rate of Optical and Electrical ports cannot be changed while circuits are provisioned on them.
EID-6288	The BERT configuration is invalid.	Refer to the eror message text.
EID-6289	The BERT mode is not yet configured	Refer to the error message text.
WID-6290	The BERT mode is configured in unframed format	Refer to the error message text.
WID-6291	Port has circuits; configuring the BERT mode will disrupt normal traffic.	Refer to the error message text.
EID-6292	The alarm type name cannot exceed 20 characters	Refer to the error message text.
EID-6294	The alarm type name contains invalid characters. Only the following characters are valid: 0-9, A-z, a-z and "-".	Refer to the error message text.
EID-6295	The alarm type is in use and cannot be deleted.	Refer to the error message text.
EID-6296	Maximum number of alarm types that can be added cannot exceed 50.	Refer to the error message text.
EID-6297	Hard coded alarm types cannot be deleted.	Refer to the error message text.
EID-6298	The alarm type already exists.	Refer to the error message text.
EID-6299	The alarm type does not exist.	Refer to the error message text.
EID-6300	Selective auto negotiation is allowed only when selected speed and duplex modes are non-auto. Click "Reset" to revert the changes.	Refer to the error message text.
WID-6301	Selective auto negotiation applies only to copper SFPs.	Refer to the error message text.
EID-6302	Users are not allowed to perform this operation.	When logged in as a maintainence user provisioning operation is not allowed.
EID-6303	The ITU-T G.709 configuration cannot be disabled when Fast Protection is enabled.	Refer to the error message text.
EID-6304	Users are not allowed to perform this operation.	Refer to the error message text.
EID-6305	The view could not be deleted.	Refer to the error message text.
EID-6306	The ITU-T G.709 configuration cannot be disabled when Fast Protection is enabled.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-6307	You have only selected one trunk-to-trunk patchcord. For complete deletion, you must select both patchcords that are attached to the 10GE_XP/GE_XP cards. Do you want to continue?	Refer to the warning message text.
WID-6308	You have only selected one trunk-to-OCH patchcord. For complete deletion, you must select both patchcords that are attached to the TXP/MXP card. Do you want to continue?	Refer to the warning message text.
EID-6309	OCHNC circuits, OSC terminations, synchronization sources and protection groups must be removed before you can remove this patchcord.	Refer to the error message text.
EID-6310	The Committed Info Rate value must be in range [0-100].	Refer to the error message text.
EID-6311	The MTU value must be in range [64-9700].	Refer to the error message text.
EID-6312	The multicast IP address must be in range [224.0.0.0 - 239.255.255.255] Exluding the following IP address subranges [(224-239).(0/128).0.(0-255)]	Refer to the error message text.
EID-6313	The multicast IP address count must be in range [1-256]	Refer to the error message text.
EID-6314	Could not retrieve TTY session for the chosen CRS.	Refer to the error message text.
EID-6315	CRS provisioning failed. {0}	Refer to the error message text.
EID-6316	The chosen node is not a CRS-1.	Refer to the error message text.
EID-6317	The value specified for IPv6 Address or IPv6 Default Router is invalid.	Refer to the error message text.
EID-6318	The value specified for Prefix Length is invalid. Valid range of values is 0 to 128.	Refer to the error message text.
EID-6319	IPv6 mode can be enabled only if SOCKS and firewall are enabled on the node.	Refer to the error message text.
EID-6320	IPv6 mode cannot be enabled on a node if RIP is enabled.	Refer to the error message text.
EID-6321	IPv6 mode cannot be enabled on a node if 'OSPF on LAN' is enabled.	Refer to the error message text.
EID-6322	IPv6 Address cannot be specified for {0} when IPv6 mode is not enabled on the node.	Refer to the error message text.
EID-6323	CTC was unable to delete SnmpV3 Target.	Refer to the error message text.
EID-6324	The card mode is invalid in this configuration.	Refer to the error message text.
EID-6325	SW version mismatch on node {0}: found {1}, expected {2}.	Refer to the error message text.
EID-6326	The CRS node {0} version[{1}] is greater than the supported version[{2}]. The creation of ochtrail circuits between CRS nodes will not be disabled, but there could be unexpected behaviours.	Refer to the error message text.
EID-6327	The end point of patchcord have an incompatible wavelength.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6329	Protection/AIS action cannot be both set to squelch.	Refer to the error message text.
EID-6330	The node failed to restart the Pseudo IOS CLI service on the selected port. Try using another unreserved port that is not being used within the 1024 - 65535 range.	Refer to the error message text.
EID-6331	That port is already in use. Also note that the Pseudo IOS port may not be changed if any Pseudo IOS connections are currently open.	Refer to the error message text.
WID-6332	All previously configured IPv6 destinations will become unreachable if IPv6 mode is disabled. It is recommended that you remove all IPv6 related provisioning before disabling IPv6 mode. Do you want to continue?	Refer to the warning message text.
WID-6333	The NE default {0} not available in the selected NE Defaults Tree.	Refer to the warning message text.
WID-6334	Could not find the NE default {0}.	Refer to the warning message text.
WID-6335	CTC was unable to create a new Target account.	Refer to the warning message text.
WID-6336	Changing the card to EFEC mode will cause the ports 1 and 2 to be disabled. Do you want to continue?	Refer to the warning message text.
WID-6337	CE-MR-10/CE-MR-6 card does not validate the Ethernet FCS when traffic is received from optical side. This can result in errored frames from optical side being forwarded to the peer device via front ports. It would be left to the peer device to detect the errors and discard the frames. It is suggested to enable the FCS option on both ends of the circuit. The GFP FCS will be used to discard errored frames. The discarded frames will be accounted under the performance pane for the POS port.	Refer to the warning message text.
WID-6338	Ingress COS setting is not compatible with QinQ mode.	Refer to the warning message text.
WID-6339	Some circuits may become partial as part of this upgrade and would need to be reconfigured.	Refer to the warning message text.
WID-6340	One or more QinQ rules have not been deleted because they are not related to the current circuit.	Refer to the warning message text.
WID-6341	The Functional view on {0} is disabled.	Refer to the warning message text.
WID-6342	Changing the {0} settings might be traffic affecting. Do you want to continue?	Refer to the warning message text.
WID-6343	The selected file name is too long. File names (including the full path) must be less than 254 characters.Please enter a valid file name.	Refer to the warning message text.
EID-6344	It is detected a shelf mismatch condition.	Refer to the error message text.
EID-6345	The line termination is invalid.	Refer to the error message text.
EID-6346	The overhead is not supported.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6347	A patchcord was expected for a successful operation.	Refer to the error message text.
EID-6348	A Virtual link already exists on the same path.	Refer to the error message text.
EID-6349	The overhead creation has failed.	Refer to the error message text.
EID-6350	The unprotected line is not present	Refer to the error message text.
EID-6351	The port status is active.	Refer to the error message text.
EID-6352	IPv4 access cannot be disabled when IPv6 mode is not enabled on the node.	Refer to the error message text.
EID-6353	IPv4 access cannot be disabled when the node is in Multishelf configuration.	Refer to the error message text.
EID-6354	Disabling IPv4 access may lead to loss of commmunication with the node. Make the change anyway?	Refer to the error message text.
EID-6355	IPv6 access cannot b disabled when IPv4 Access is disabled on the node.	Refer to the error message text.
EID-6356	Multishelf configuration cannot be enabled when IPv4 Access is disabled on the node.	Refer to the error message text.
EID-6357	The Multicast SVLAN field can be modified only when the MVR feature is disabled.	Refer to the error message text.
EID-6358	Too many TRANSLATE QinQ rules per port with MVR feature enabled.	Refer to the error message text.

1. EID-3159 can appear if you attempt to perform another switching operation within a certain time interval. This interval is an algorithm of three seconds per working card in the protection group. The maximum interval is 10 seconds.

INDEX

Numerics

1+1 optical port protection, deleting 2-82
15310-CL-CTX card
  line alarms 2-155
  resetting 2-162
15xxx RR handheld receiver
  See also electrical wiring verification
  automatic mode tests 1-59
  default 1-59
  manual mode tests 1-57
  usage flow chart 1-56

A

ADMIN-DISABLE 3-4
ADMIN-DISABLE-CLR 3-4
ADMIN-LOCKOUT 3-4
ADMIN-LOCKOUT-CLR 3-4
ADMIN-LOGOUT 3-5
ADMIN-SUSPEND 3-5
ADMIN-SUSPEND-CLR 3-5
AIS
  AIS-L 2-21
  AIS-P 2-21
  AIS-V 2-22
  AIS-V on unused VT circuits 1-82
  AUTOSW-AIS 2-31
  FE-AIS 2-63
  TX-AIS 2-150
alarms
  See individual alarm names
  alphabetical list 2-6
  characteristics 2-16
  frequently used troubleshooting procedures 2-156
  hierarchy 2-17
  list arranged by logical object type 2-12
  list of Critical 2-2
  list of Major 2-2
  list of Minor 2-3
  list of Not-Alarmed conditions 2-4
  list of Not Reported conditions 2-6
  logical objects 2-10
  service effect 2-19
  severities 2-17
  state
    C 2-19
    R 2-19
    T 2-19
  TL1 2-1
  trouble notifications 2-16
  troubleshooting 2-1 to 2-167
alignment, loss of 2-91
ALS 2-22
AMI coding 2-93, 2-94
APC-END 2-22
APS. *See* automatic protection switching
APSB 2-22
APSCDFLTK 2-23
APSCINCON 2-23
APSCM 2-23
APSCNMIS 2-24
APSIMP 2-24
APS-INV-PRIM 2-25
APSMM 2-25
APS-PRIM-FAC 2-27

APS-PRIM-SEC-MISM 2-27
AS-CMD 2-27
AS-MT 2-29
AS-MT-OOG 2-29
asynchronous mapping 2-123
AUD-ARCHIVE-FAIL 3-5
AUD-LOG-LOSS 2-29
AUD-LOG-LOW 2-30
AUTOLSROFF 2-30
automatic protection switching
  byte failure 2-22
  channel failure on protect card 2-69
  channel mismatch 2-23
  FEPRLF 2-69
  mode mismatch failure 2-25
  path protection 2-31, 2-32, 2-33, 2-34
  SWMTXMOD-PROT 2-142
  SWMTXMOD-WORK 2-142
automatic reset 2-30
AUTORESET 2-30
AUTOSW (STSMON) 2-32
AUTOSW-AIS 2-31
AUTOSW-LOP (STSMON) 2-32
AUTOSW-LOP (VT-MON) 2-32
AUTOSW-PDI 2-32
AUTOSW-SDBER 2-33
AUTOSW-SFBER 2-33
AUTOSW-UNEQ (STSMON) 2-34
AUTOSW-UNEQ (VT-MON) 2-34

B

B8ZS coding 2-93, 2-94
BAT-FAIL 2-35
battery
  extreme high voltage alarm 2-52
  extreme low voltage alarm 2-52
  high voltage alarm 2-76
  low voltage alarm 2-113
  LWBATVG 2-113
BER
  AUTOSW-SDBER 2-33
  AUTOSW-SFBER 2-33
  SD 2-130
  SD-L 2-132
  SD-P 2-133
  SD-V 2-133
  SF 2-134
  SF-L 2-134
  SF-P 2-135
  SF-V 2-135
BER, verifying threshold level 2-164
BERT-SYNC-FAIL 2-36
bidirectional protection 2-69
bit error rate. *See* BER
BITS
  daisy-chained 1-85
  errors 1-84, 1-85
  loss of frame 2-92
  loss of framing 2-92
  loss of signal 2-101
  source failure 2-72
BKUPMEMP 2-36
browser
  cannot launch CTC after removing Netscape 1-69
  cannot launch Java 1-66
  reconfiguring 1-67
  stalls during download 1-71
  supported by CTC 1-64
  unsupported in this release 1-65
BSLROSYNC 2-37

C

C2 byte 2-53
cache
  deleting 1-73
  redirecting 1-72

calculating IP subnets 1-80
CARLOSS
CARLOSS (ML100T) 2-40
CE-100T-8 card 2-37
CE100T-8 card 2-37
CE-MR-6 card 2-37
equipment 2-39
carrier loss 2-37, 2-39
CAT-5 cable. *See* LAN cable
CE-100T-8 card
replacing 2-163
reseating 2-163
resetting 2-162
CE-Series Ethernet cards
carrier loss 2-37
changing
IP address 2-51
timing reference 2-82
circuits
AIS-V condition 1-82
circuit state transition error 1-80
deleting 2-164
generic procedures 2-164
identifying circuit state 1-81
identifying failure points on electrical 1-3
identifying failure points on optical 1-16
PARTIAL status remains unchanged 1-81
path-in-use error 1-79
repairing 1-81
rolled 2-128
roll pending 2-129
VT1.5 creation error 1-83
CLDRESTART 2-41
clearing
1+1 Force or Manual switch 2-158
alarms. *See* individual alarm names
conditions. *See* individual condition names
DS-3 or DS-1 port loopback circuit 2-165
EC-1 port loopbacks 2-166
Ethernet facility loopback circuit 1-46
Ethernet loopback circuit 2-166
Ethernet terminal loopback circuit 1-35, 1-49
facility loopback circuit 1-32
lock-on or lockout 2-159
OC-N port cross-connect loopback circuit 2-165
OC-N port facility loopback circuit 1-40, 2-165
OC-N port terminal loopback circuit 2-165
OC-N terminal loopback circuit 1-43
path protection span switch 2-161
cold restart 2-41
COMIOXC 2-42
conditions
See individual condition names
See also individual transient names
characteristics 2-16
list of Not-Alarmed 2-4
list of Not Reported 2-6
CONTBUS-CLK-A 2-43
CONTBUS-CLK-B 2-43
CONTBUS-DISABLED 2-44
CONTBUS-IO-A 2-45
CONTBUS-IO-B 2-45
controller card
LED behavior after insertion 2-156
testing 1-41, 1-44
correcting the CTC core version build 1-76
CRC 2-36, 2-53, 2-87
DATA-CRC 2-48
creating
cross-connect loopback on a source-node OC-N port 1-18
DCC terminations 2-164
facility loopback on a destination-node electrical port 1-14
facility loopback on a destination-node Ethernet port 1-45
facility loopback on a destination-node OC-N port 1-24

facility loopback on an intermediate-node OC-N port 1-21, 1-39
facility loopback on a source-node electrical port 1-4
facility loopback on a source-node Ethernet port 1-31
facility loopback on a source-node OC-N port 1-17
hairpin on a destination-node electrical port 1-13
hairpin on a source-node electrical port 1-6
terminal loopback on a destination-node electrical port 1-7, 1-10
terminal loopback on a destination-node Ethernet port 1-48
terminal loopback on a destination-node OC-N port 1-26
terminal loopback on an intermediate-node OC-N port 1-23, 1-42
terminal loopback on a source-node Ethernet port 1-33
terminal loopback on a source-node OC-N port 1-19
crimping LAN cables 1-88
cross-connect alarms
COMIOXC 2-42
CTNEQPT-PBPROT 2-46
LPBKCRS 2-108
cross-connect cards
test during a hairpin circuit 1-38, 1-52, 1-53
cross-connect loopback
clearing on an OC-N port 2-165
creating on a source-node OC-N port 1-18
definition 1-3
LPBKCRS 2-108
performing on a source-node OC-N port 1-18
testing 1-19
testing an optical circuit 1-16
using to test an Ethernet circuit path 1-31
using to test an optical circuit path 1-16
CTC
applet not loaded 1-66
correcting the core version build 1-76
deleting cache files 1-73
does not launch 1-72
gray node icon 1-74
list of alarms 2-1
login errors 1-66, 1-71, 1-77
loss of TCP/IP connection 2-39
node view to network view change unsuccessful 1-70
release interoperability problems 1-76
requirements for UNIX workstation 1-64
requirements for Windows PC 1-64
setting Internet Explorer as the default browser 1-70
sluggish operation 1-73
supported platforms, browsers, and JREs 1-64
troubleshooting operation 1-69
unable to launch 1-69
username and password mismatch 1-77
verifying PC connection 1-68
CTNEQPT-PBPROT 2-46
CTNEQPT-PBWORK 2-47
CTX2500 card
communication failure between protect and traffic card 2-46
reseating 2-163
resetting 2-162
cyclic redundancy checking 2-36

D

database
memory exceeded 2-49
restoring 1-63
standby not synchronized with the active 2-49
DATA-CRC 2-48
DATAFLT 2-48
DBBACKUP-FAIL 3-5
DBOSYNC 2-49
DBRESTORE-FAIL 3-5
DCC
connection loss 1-79
creating DCC terminations 2-164
deleting DCC terminations 2-82

limitations with OC-3 1-83
two-DCC requirement during facility loopback 1-2
verifying DCC terminations 2-164
deleting
circuits 2-164
CTC cache 1-73
DCC terminations 2-82
protection groups 2-82
designing IP subnets 1-80
diagnostic tests
retrieve 1-92
DISCONNECTED 1-68, 2-49
downloading software 2-135
DS1-28/DS3-EC1-3 card
line alarms 2-155
replacing 2-163
reseating 2-163
resetting 2-162
DS1-84/DS3-EC1-3 card
line alarms 2-155
replacing 2-163
reseating 2-163
resetting 2-162
DS-3 frame format mismatch 2-50
DS3-MISM 2-50
DSX wiring panel 1-54
DUP-IPADDR 2-50
DUP-NODENAME 2-51
DUP-SHELF-ID 2-52

E

EC1
LOF 2-95
LOS 2-104
LPBKFACILITY 2-110
LPBKTERMINAL 2-112
EFM-ERR-FRM 3-6
EFM-FRM-PER 3-6
EFM-FRM-SEC 3-6
EFM-RLBK-FAIL 3-6
EFM-SYM-PER 3-6
EHIBATVG 2-52
electrical cables
See also electrical wiring verification
test during a facility loopback 1-6, 1-16
electrical card
See also DS1-28/DS3-EC1-3 card
See also DS1-84/DS3-EC1-3 card
resetting 2-162
electrical wiring verification
automatic mode test 1-59
automatic test results 1-61
description 1-54
loop tests 1-62
manual mode tests 1-57
set up equipment 1-54
troubleshoot manual tests 1-58
ELWBATVG 2-52
ENCAP-MISMATCH-P 2-53
EOC 2-54
EOC-L 2-56
EQPT
CARLOSS 2-39
EQPT alarm 2-57
EQPT-MISS 2-58
FE-EQPT-NSA 2-67
MEA 2-116
equipment failure
hardware failure on reporting card 2-57
missing or failed fan tray 2-58
ERFI-P-CONN 2-58
ERFI-P-PAYLD 2-59
ERROR-CONFIG 2-59
error messages 4-1 to 4-53
ESF 2-155
Ethernet
create a hairpin circuit 1-37, 1-51

Ethernet cards
LED behavior after insertion 2-156
resetting 2-162
testing 1-32, 1-35, 1-47, 1-50
ETH-LINKLOSS 2-60
EXCCOL 2-61
EXT 2-61
external switching commands
clearing a 1+1 Force or Manual switch 2-158
clearing a lock-on or lockout 2-159
clearing a path protection span switch 2-161
initiating a 1+1 Manual switch 2-157
initiating a 1+1 protection port Force switch 2-157
initiating a 1:1 card switch command (ONS 15310-MA only) 2-159
initiating a lock-on 2-158
initiating a lockout 2-159
initiating a path protection Force switch 2-160
initiating a path protection lockout 2-161
initiating a path protection Manual switch 2-160

F

facility loopback
clearing an Ethernet circuit 1-46
clearing anOC-N circuit 1-40
clearing circuit 1-32
creating on a destination-node electrical port 1-14
creating on a destination-node Ethernet port 1-45
creating on a destination-node OC-N port 1-24
creating on an intermediate-node OC-N port 1-21, 1-39
creating on a source-node electrical port 1-4
creating on a source-node Ethernet port 1-31
creating on a source-node OC-N port 1-17
definition 1-2
LPBKFACILITY (CE100T, CEMR) 2-109
LPBKFACILITY (DS1, DS3) 2-109
LPBKFACILITY (EC1) 2-110
LPBKFACILITY (OCN) 2-111
performing on a destination-node Ethernet port 1-45
performing on a destination-node OC-N port 1-24
performing on an intermediate-node OC-N port 1-21
performing on an intermediate-node OC-N port during an Ethernet circuit test 1-39
performing on a source-node Ethernet port 1-31
performing on a source-node OC-N port 1-17
perform on a source-node electrical port 1-4
testing 1-5, 1-15, 1-17, 1-22, 1-25, 1-32
testing an electrical circuit 1-4
testing an Ethernet circuit 1-46
testing an OC-N circuit 1-40
testing an optical circuit 1-16
using to test an electrical circuit path 1-3
using to test an Ethernet circuit path 1-31
using to test an optical circuit path 1-16
FAILTOSW 2-62
FAILTOSW-PATH 2-62
fan alarms
EQPT-MISS 2-58
FAN alarm 2-63
FAN-DEGRADE 2-63
MEA 2-117
MFGMEM 2-118
fan tray, missing or failed 2-58
FE-AIS 2-63
FE-DS1-MULTLOS 2-64
FE-DS1-NSA 2-64
FE-DS1-SA 2-65
FE-DS1-SNGLLOS 2-65
FE-DS3-NSA 2-66
FE-DS3-SA 2-66
FE-EQPT-NSA 2-67
FE-FRCDWKSWBK-SPAN 2-67
FE-FRCDWKSWPR-SPAN 2-68
FE-IDLE 2-68
FE-LOCKOUTOFPR-SPAN 2-68
FE-LOF 2-68

FE-LOS 2-69
FE-MANWKSWBK-SPAN 2-69
FE-MANWKSWPR-SPAN 2-69
FEPRLF 2-69
fiber and cabling errors 1-86
fiber-optic connections
faulty 1-86
firewall, invalid port number 4-12
FIREWALL-DIS 3-6
flash manager 2-36
flash memory, capacity exceeded 2-49
flow rate 2-61
FORCED-REQ 2-70
FORCED-REQ-SPAN 2-70
Force switch. *See* external switching commands
FP-LINK-LOSS 2-71
frame, loss of 2-150
framing, loss of 2-92, 2-93, 2-94, 2-95, 2-96
FRCDSWTOINT 2-71
FRCDSWTOPRI 2-71
FRCDSWTOSEC 2-71
FRCDSWTOTHIRD 2-72
FRCDWKSWBK-NO-TRFSW 3-7
FRCDWKSWPR-NO-TRFSW 3-7
free running synchronization 1-85, 2-72
FRNGSYNC 1-85, 2-72
FSTSYNC 2-72
FUDC
LOS 2-105
FULLPASSTHR-BI 2-73

G

GFP
failure, indicated by ENCAP-MISMATCH-P 2-53
GFP-CSF 2-73
GFP-EX-MISMATCH 2-73
GFP-LFD 2-74
GFP-UP-MISMATCH 2-74

H

hairpin circuit
creating on a destination-node electrical port 1-13
creating on a source-node electrical port 1-6
definition 1-3
performing on a destination-node electrical port 1-13
performing on a source-node electrical port 1-6
perform on a destination-node Ethernet port 1-51
testing 1-7, 1-14
testing an electrical circuit 1-4
using to test an electrical circuit path 1-3
half-duplex 2-61
handheld receiver. *See* 15xxx RR handheld receiver
hard reset 2-162
HDLC 2-48
failure, indicated by ENCAP-MISMATCH-P 2-53
HELLO 2-75
HIBATVG 2-76
HI-LASERBIAS 2-76
HI-LASERTEMP 2-77
HI-RXPOWER 2-78
HITEMP 2-78
HI-TXPOWER 2-78
HLDOVRSYNC 1-84, 2-79
holdover synchronization 2-79

I

identifying
circuit states 1-81
failure points on electrical circuits 1-3
failure points on optical circuits 1-16
idle signal condition 2-68
I-HITEMP 2-80
improper card removal 2-81
IMPROPRMVL 2-81
INC-ISD 2-82
INCOMPATIBLE-SEND-PDIP 2-83

INCOMPATIBLE-SW 1-76, 2-83
INHSWPR 2-83
INHSWWKG 2-84
initiating
1+1 Manual switch 2-157
1+1 protection port Force switch 2-157
1:1 card switch (ONS 15310-MA only) 2-159
lock-on 2-158
lockout 2-159
path protection Force switch 2-160
path protection lockout 2-161
path protection manual switch 2-160
Internet Explorer
See also browser
setting as the default CTC browser 1-70
interoperability between CTC releases 1-76
INTRUSION 3-7
INTRUSION-PSWD 2-84, 3-7
INVMACADR 2-85
IOS
ERROR-CONFIG 2-59
IOSCFGCOPY 2-85
NO-CONFIG 2-119
RUN-CFG-SAVENEED 2-130
IP address
changing 2-51
no connectivity between nodes 1-78
same address assigned twice in a DCC area 2-51
unsuccessful ping 1-65
IP subnets, cannot calculate or design 1-80
ISIS-ADJ-FAIL
OSI routing 2-85

J

Java
browser will not launch 1-66
Java Runtime Environment. *See* JRE
reconfiguring Java plug-in control panel 1-66
JRE
cannot launch 1-66
description 1-75
incompatibility 1-75
launch failure 1-66
unsupported in this release 1-65
versions supported by CTC 1-64

K

KB-PASSTHR 2-87

L

lamp test 1-91
LAN cable
crimping 1-88
damaged cable 1-68
faulty cable 1-86
laser alarms
HI-LASERBIAS 2-76
HI-LASERTEMP 2-77
LASEREOL 2-87
LO-LASERBIAS 2-97
LO-LASERTEMP 2-98
laser transceiver temperature 2-77
LCAS 2-88
LCAS-CRC 2-87
LCAS-RX-DNU 2-88
LCAS-RX-FAIL 2-89
LCAS-TX-ADD 2-89
LCAS-TX-DNU 2-90
LCAS-CRC 2-87
LCAS-RX-FAIL 2-89
LCAS-TX-ADD 2-89
LCAS-TX-DNU 2-90
LDCC 2-56
LED operation

blinking STAT LED 1-85
lamp test 1-91
typical activity 2-156
line coding 2-93
line framing 2-93, 2-94
line interface unit 1-2
LINK-KEEPALIVE 2-90
LKOUTPR-S 2-91
LOA 2-91
lock initiation 2-156
lock-on. *See* external switching commands
lockout. *See* external switching commands
LOCKOUT-REQ 2-92
LOF
FE-LOF 2-68
LOF (BITS) 2-92
LOF (DS1) 2-93
LOF (DS3) 2-94
LOF (EC1) 2-95
LOF (OCN) 2-95
LOF (STSTRM) 2-96
TX-LOF 2-150
log alarms
LOGBUFR90 2-96
LOGBUFROVFL 2-96
login errors
browser login does not launch Java 1-66
browser stalls when downloading JAR file 1-71
corrupt cache file 1-73
CTC does not launch 1-72
no DCC connection 1-79
no IP connectivity 1-78
username/password mismatch 1-77
LOGIN-FAILURE-LOCKOUT 3-7
LOGIN-FAILURE-ONALRDY 3-7
LOGIN-FAILURE-PSWD 3-7
LOGIN-FAILURE-USERID 3-8
LOGOUT-IDLE-USER 3-8
LO-LASERBIAS 2-97
LO-LASERTEMP 2-98
LOM 2-98
loopback
See also cross-connect loopback
See also facility loopback
See also terminal loopback
clearing a DS-1 or DS-3 port loopback 2-165
clearing an EC-1 port loopback 2-166
clearing an Ethernet card loopback 2-166
description 1-2
loopback alarms
LPBKCRS 2-108
LPBKDS3FEAC 2-108
LPBKDS3FEAC-CMD 2-109
LPBKFACILITY (CE100T, CEMR) 2-109
LPBKFACILITY (DS1, DS3) 2-109
LPBKFACILITY (EC1) 2-110
LPBKFACILITY (OCN) 2-111
LPBKTERMINAL (CE100T, CEMR) 2-111
LPBKTERMINAL (DS1, DS3) 2-112
LPBKTERMINAL (EC1) 2-112
LPBKTERMINAL (OCN) 2-113
LOP
AUTOSW-LOP (STSMON) 2-32
AUTOSW-LOP (VT-MON) 2-32
LOP-P 2-98
LOP-V 2-99
LO-RXPOWER 2-99
LOS
FE-LOS 2-69
LOS (BITS) 2-101
LOS (DS1) 2-101
LOS (DS3) 2-102
LOS (EC1) 2-104
LOS (FUDC) 2-105
LOS (OCN) 2-106
loss of pointer. *See* LOP
loss of signal. *See* LOS
LO-TXPOWER 2-107

LPBKCRS 2-108
LPBKDS3FEAC 2-108
LPBKDS3FEAC-CMD 2-109
LPBKFACILITY
LPBKFACILITY (CE100T, CEMR) 2-109
LPBKFACILITY (DS1, DS3) 2-109
LPBKFACILITY (EC1) 2-110
LPBKFACILITY (OCN) 2-111
LPBKTERMINAL
CE100T-8 card 2-111
CEMR-6 card 2-111
LPBKTERMINAL (DS1) 2-112
LPBKTERMINAL (EC1) 2-112
LPBKTERMINAL (OCN) 2-113
LWBATVG 2-113

M

MAC address, invalid 2-85
MAN-REQ 2-114
MANRESET 2-114
MANSWTOINT 2-114
MANSWTOPRI 2-114
MANSWTOSEC 2-115
MANSWTOTHIRD 2-115
MANUAL-REQ-SPAN 2-115
MANWKSWBK-NO-TRFSW 3-8
MANWKSWPR-NO-TRFSW 3-8
MATECLK 2-116
MEA
MEA (EQPT) 2-116
MEA (FAN) 2-117
MEA (PPM) 2-118
MEA (SHELF) 2-118
MEM-GONE 2-118
MEM-LOW 2-118
memory alarms
BKUPMEMP 2-36
DATAFLT 2-48
MEM-GONE 2-118
MEM-LOW 2-118
MFGMEM 2-118
mismatch between received and expected C2 byte 2-53
ML-100T-8 card
CARLOSS 2-40
replacing 2-163
reseating 2-163
resetting 2-162
startup configuration error 2-59
modifying. *See* changing
multiframe, loss of 2-98

N

Netscape Navigator
See also browser
clear cache 1-72
network view, gray node icon 1-74
NIC card
cannot verify 1-67
removing 1-67
NO-CONFIG 2-119
node view, cannot change to network view 1-70
NON-CISCO-PPM 2-119
NOT-AUTHENTICATED 1-77, 2-120

O

OC-N alarms
AIS-L 2-21
APSB 2-22
APSCINCON 2-23
APSCM 2-23
APSIMP 2-24
APS-INV-PRIM 2-25
APSMM 2-25
APS-PRIM-FAC 2-27

APS-PRIM-SEC-MISM 2-27
AS-CMD 2-27
AS-MT 2-29
EOC 2-54
EOC-L 2-56
FAILSTOSW 2-62
FE-FRCWKSWBK-SPAN 2-67
FEPRLF 2-69
FORCED-REQ-SPAN 2-70
HELLO 2-75
HI-TXPOWER 2-78
LKOUTPR-S 2-91
LOCKOUT-REQ 2-92
LOF 2-95
LO-RXPOWER 2-99
LOS 2-106
LO-TXPOWER 2-107
LPBKFACILITY 2-111
LPBKTERMINAL 2-113
MANUAL-REQ-SPAN 2-115
RFI-L 2-126
SD-L 2-132
SF-L 2-134
SSM-DUS 2-137
SSM-FAIL 2-137
SSM-OFF 2-138
SSM-PRS 2-139
SSM-RES 2-139
SSM-SMC 2-139
SSM-ST2 2-140
SSM-ST3 2-140
SSM-ST3E 2-140
SSM-ST4 2-140
SSM-STU 2-141
SSM-TNC 2-141
SYNC-FREQ 2-144
TIM 2-146
TIM-MON 2-147
TIM-S 2-148
WKSWPR 2-155
WTR 2-155
OC-N ports
bit errors 1-86
clearing a loopback 2-165
OC-3 and DCC limitations 1-83
OOU-TPT 2-120
OPEN-SLOT 2-120
optical power alarms
HI-RXPOWER 2-78
HI-TXPOWER 2-78
LO-RXPOWER 2-99
LO-TXPOWER 2-107

P

password
incorrect 2-84
mismatch with username 1-77
resetting for Superuser 1-77
verifying 1-77
path protection
LOP 2-32
path protection alarms 2-31, 2-32
path protection configurations
clearing span switch 2-161
initiating a Force switch for all circuits on the span 2-160
initiating a lockout for all circuits on a protect span 2-161
initiating a Manual switch for all circuits on the span 2-160
signal failure alarm 2-33
payload mismatch, GFP ports 2-74
PC connectivity 1-63
PDI
AUTOSW-PDI 2-32
INCOMPATIBLE-SEND-PDIP 2-83
PDI-P 2-121

Ping 2-136
ping 1-65, 1-68, 1-69, 2-40, 2-136
platform
unsupported in this release 1-65
PLM
PLM-P 2-122
PLM-V 2-123
PM-TCA 3-8
PORT-MISMATCH 2-123
power
See also battery
cannot power up node or cards 1-91
supply problems 1-90
power alarms
BAT-FAIL 2-35
EHIBATVG 2-52
ELWBATVG 2-52
HIBATVG 2-76
LWBATVG 2-113
PWR-FAIL-A 2-125
PWR-FAIL-B 2-125
PPM alarms
AD-CMD 2-27
AS-MT 2-29
EQPT 2-57
HI-LASERBIAS 2-76
HI-LASERTEMP 2-77
HI-TXPOWER 2-78
IMPROPRMVL 2-81
LO-LASERBIAS 2-97
LO-TXPOWER 2-107
MEA 2-118
MFGMEM 2-118
NON-CISCO-PPM 2-119
UNQUAL-PPM 2-153
PRC-DUPID 2-124
protection group, deleting 2-82
PROTNA 2-124
PROV-MISMATCH 2-124
PS 3-8
PWR-FAIL-A 2-125
PWR-FAIL-B 2-125

R

RAI 2-126
TX-RAI 2-151
receiver, for testing wiring *See* 15xxx RR handheld receiver 1-57
reconfiguring
browsers 1-67
Java plug-in control panel 1-66
redirecting the CTC cache 1-72
removing the NIC card 1-67
repairing circuits 1-81
replacing cards 2-163
reseating cards 2-163
resetting
controller cards 2-162
electrical cards 2-162
Ethernet cards 2-162
Superuser password 1-77
restoring the node database 1-63
RFI
ERFI-P-CONN 2-58
ERFI-P-LAYLD 2-59
RFI-L 2-126
RFI-P 2-127
RFI-V 2-127
RMON-ALARM 3-9
RMON-RESET 3-9
ROLL 2-128
ROLL-PEND 2-129
RPR 2-48
RPR-PASSTHR 2-129
RPRW 2-129
RUN-CFG-SAVENEED 2-130

S

safety
- warnings 2-19

safety information 2-19

SD 2-130
- AUTOSW-SDBER 2-33
- SD-L 2-132
- SD-P 2-133
- SD-V 2-133

SDCC
- termination failure 2-54

security alarms
- INTRUSION-PSWD 2-84

SESSION-TIME-LIMIT 3-9

setting the default CTC browser 1-70

severities, alarm 2-17

SF 2-134
- AUTOSW-SFBER 2-33
- SF-L 2-134
- SF-P 2-135
- SF-V 2-135

SFTWDOWN 2-135

SFTWDOWN-FAIL 3-9

SHELF-COMM-FAIL 2-136

signal, loss of 2-101, 2-102, 2-104, 2-105, 2-106

signal failure 2-134

SNTP-HOST 2-136

soft reset 2-162

software download 2-135

SQM 2-137

SSM
- degrade 2-137
- failure 2-138
- SSM-DUS 2-137
- SSM-FAIL 2-137
- SSM-LNC 2-138
- SSM-OFF 2-138
- SSM-PRC 2-138
- SSM-PRS 2-139
- SSM-RES 2-139
- SSM-SDN-TN 2-139
- SSM-SETS 2-139
- SSM-SMC 2-139
- SSM-ST2 2-140
- SSM-ST3 2-140
- SSM-ST3E 2-140
- SSM-ST4 2-140
- SSM-STU 2-141
- SSM-TNC 2-141
- timing switch 1-84

STM-N alarms
- SSM-PRC 2-138

switching
- *See* automatic protection switching
- *See* external switching commands

switching alarms
- FAILTOSW 2-62
- FAILTOSW-PATH 2-62
- FE-FRCDWKSWBK-SPAN 2-67
- FE-FRCDWKSWPR-SPAN 2-68
- FE-LOCKOUTOFPR-SPAN 2-68
- FE-MANWKSWBK-SPAN 2-69
- FE-MANWKSWPR-SPAN 2-69
- FORCED-REQ 2-70
- FORCED-REQ-SPAN 2-70
- INHSWPR 2-83
- INHSWWKG 2-84
- LKOUTPR-S 2-91
- LOCKOUT-REQ 2-92
- MAN-REQ 2-114
- MANUAL-REQ-SPAN 2-115
- PROTNA 2-124
- WKSWPR 2-155

SWMTXMOD-PROT 2-142

SWTOPRI 2-143

SWTOSEC 2-143

SWTOTHIRD 2-143

SYNC-FREQ 2-144
synchronization alarms
DBOSYNC 2-49
FRNGSYNC 2-72
FSTSYNC 2-72
HLDOVRSYNC 2-79
SSM-DUS 2-137
SSM-FAIL 2-137
SSM-LNC 2-138
SSM-OFF 2-138
SSM-RES 2-139
SSM-SETS 2-139
SSM-SMC 2-139
SSM-ST2 2-140
SSM-ST3 2-140
SSM-ST3E 2-140
SSM-ST4 2-140
SSM-STU 2-141
SSM-TNC 2-141
SYNC-FREQ 2-144
SYNCPRI 2-144
SYNCSEC 2-145
SYNCTHIRD 2-145
synchronization status message. *See* SSM
SYNCPRI 2-144
SYNCSEC 2-145
SYNCTHIRD 2-145
SYSBOOT 2-146
system alarms
DISCONNECTED 2-49
INCOMPATIBLE-SEND-PDIP 2-83
NOT-AUTHENTICATED 2-120

T

TCP/IP 1-68, 2-39
Telcordia
signal degrade definition 2-130
signal failure definition 2-134
temperature alarms
FAN 2-63
FAN-DEGRADE 2-63
HI-LASERTEMP 2-77
HITEMP 2-78
I-HITEMP 2-80
LO-LASERTEMP 2-98
terminal loopback
clearing Ethernet circuit 1-35, 1-49
clearing OC-N circuit 1-43
creating on a destination-node electrical port 1-7, 1-10
creating on a destination-node Ethernet port 1-48
creating on a destination-node OC-N port 1-26
creating on an intermediate-node OC-N port 1-23, 1-42
creating on a source-node Ethernet port 1-33
creating on a source-node OC-N port 1-19
definition 1-3
LPBKTERMINAL (CE100T, CEMR) 2-111
LPBKTERMINAL (DS1, DS3) 2-112
LPBKTERMINAL (EC1) 2-112
LPBKTERMINAL (OCN) 2-113
performing on a destination-node electrical port 1-7, 1-9
performing on a destination-node Ethernet port 1-48
performing on a destination-node OC-N port 1-26
performing on an intermediate-node OC-N port 1-22
performing on an intermediate-node OC-N port during an Ethernet circuit test 1-42
performing on a source-node Ethernet port 1-33
performing on a source-node OC-N port 1-19
testing 1-20, 1-24, 1-27
testing an electrical circuit 1-4
testing an optical circuit 1-16
testing Ethernet circuit 1-35, 1-49
testing OC-N circuit 1-43
testing on a destination-node electrical port 1-9
using to test an electrical circuit path 1-3
using to test an Ethernet circuit path 1-31
using to test an optical circuit path 1-16

termination failure
LDCC 2-56
testing
See also lamp test
See also loopback
See also power
cross-connect loopback circuit 1-19
electrical cabling 1-6, 1-16
electrical circuits 1-4
Ethernet cards 1-32, 1-35, 1-47, 1-50
Ethernet facility loopback circuit 1-46
Ethernet terminal loopback circuit 1-35, 1-49
facility loopback circuit 1-5, 1-15, 1-17, 1-22, 1-25, 1-32
hairpin circuit 1-7, 1-14
LED operation 1-91
network tests 1-2 to 1-3
OC-N (controller) card 1-41, 1-44
OC-N facility loopback circuit 1-40
OC-N terminal loopback circuit 1-43
optical circuits 1-16
terminal loopback circuit 1-9, 1-20, 1-24, 1-27
TIM 2-146
TIM-MON 2-147
TIM-P 2-148
TIM-S 2-148
TIV-V 2-149
timing
free-running synchronization error 1-85
holdover error 1-84
timing alarms
CONTBUS-CLK-A 2-43
CONTBUS-CLK-B 2-43
FRCDSWTOINT 2-71
FRCDSWTOPRI 2-71
FRCDSWTOSEC 2-71
FRCDSWTOTHIRD 2-72
LOF (BITS) 2-92
LOS (BITS) 2-101
loss of primary reference 2-144
MANSWTOINT 2-114
MANSWTOPRI 2-114
MANSWTOSEC 2-115
MANSWTOTHIRD 2-115
MATECLK 2-116
SSM-PRC 2-138
SSM-PRS 2-139
SWTOPRI 2-143
SWTOSEC 2-143
SWTOTHIRD 2-143
WTR 2-155
timing reference
automatic switch to secondary source (condition) 2-143
automatic switch to third timing source (condition) 2-143
changing 2-82
manual switch to internal source (condition) 2-114
manual switch to primary source (condition) 2-115
manual switch to second source (condition) 2-115
manual switch to third source (condition) 2-115
switch error 1-83
TL1 alarms 2-1
TPTFAIL 2-149
transient conditions
See individual transient names
alphabetical list 3-1
characteristics 3-3
troubleshooting
See also loopback
alarm characteristics 2-16
alarms 2-1 to 2-167
conditions 2-16
CTC operation 1-69
frequently used procedures 2-156 to 2-167
general troubleshooting procedures 1-1 to 1-92
network tests 1-2 to 1-3
PC connectivity 1-63
severities 2-17

trouble notifications 2-16

TST-DSX card 1-54

TX-AIS 2-150

TX-LOF 2-150

TX-RAI 2-151

U

UNEQ

AUTOSW-UNEQ (STSMON) 2-34

AUTOSW-UNEQ (VT-MON) 2-34

UNEQ-P 2-151

UNEQ-V 2-153

UNQUAL-PPM 2-153

USER-LOCKOUT 3-9

USER-LOGIN 3-9

USER-LOGOUT 3-9

username/password mismatch 1-77

V

VCCG-DOWN 2-154

VCG-DEG 2-154

verifying

BER threshold level 2-164

DCC terminations 2-164

electrical connections between the ONS 15310-MA and DSX panel 1-54

passwords 1-77

Windows PC connection to the node 1-68

VirusScan

disable 1-71

disabling the download scan 1-72

voltage. *See* battery

VT1.5 creation error 1-83

W

warnings

safety summary 2-19

wiring, verify 1-54

WKSWBK 3-10

WKSWPR 2-155, 3-10

WRMRESTART 3-10

WTR 2-155